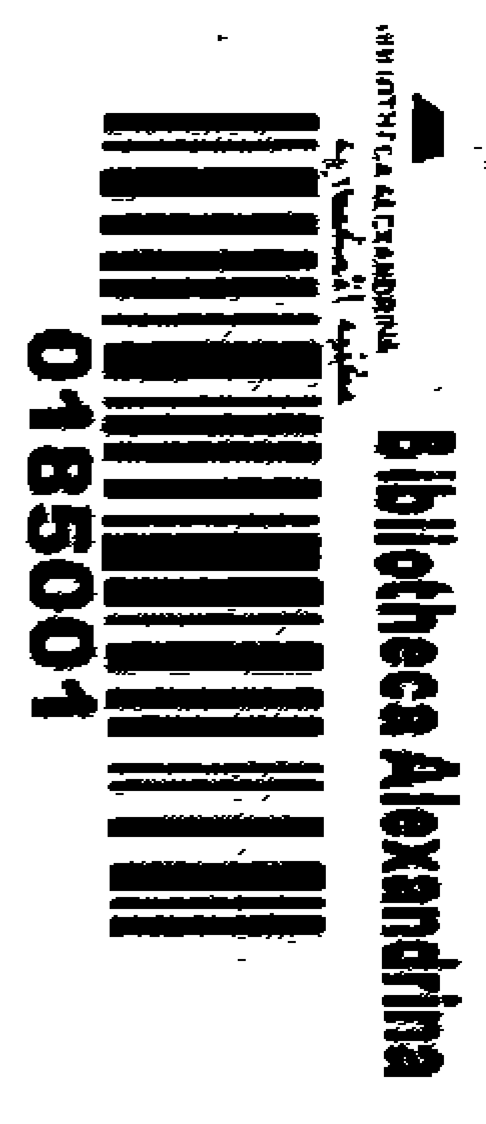
نديم عبده

الأنظمة الحديثة للمخابرات

عرض علمي وموضوعي لتقنيات المخابرات الحديثة

- النشاط المخابراتي الأميركي
- دور المخابرات في مفهوم الأمن القومي الأميركي
- الرقابة والتجسس بالأقمار الصناعية
- التنصت على الاتصالات
- معالجة بيانات التنصت
- محاولات السيطرة على الأدمغة
- التجسس في القطاع الخاص
- تقنيات التجسس في القطاع الخاص
- تشفير الاتصالات
- اعتماد الجيوش على التقنيات المدنية
- النشاط المخابراتي اليهودي



الأنظمة الحديثة
للمخابرات

نديم عبده

الأنظمة الحديثة للمخابرات

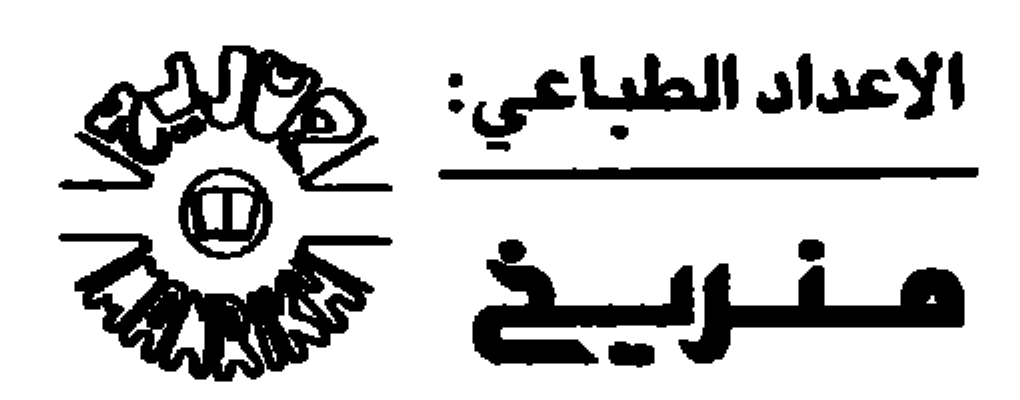
عرض علمي وموضوعي لتقنيات المخابرات الحديثة

- النشاط المخابراتي الأميركي
- دور المخابرات في مفهوم الأمن القومي الأميركي
- الرقابة والتجسس بالأقمار الصناعية
- التنصت على الاتصالات
- معالجة بيانات التنصت
- محاولات السيطرة على الأدمغة
- التجسس في القطاع الخاص
- تقنيات التجسس في القطاع الخاص
- تشفير الاتصالات
- اعتماد الجيوش على التقنيات المدنية
- النشاط المخابراتي اليهودي

صادر عن: نديم عبده
ص.ب 165903 بيروت - لبنان

طبع في سنة 1999

الاعداد الطباعي:



منريخ
للطباعة والنشر والتوزيع
هاتف: 663172

مقدمة عامة

يعتبر الحصول على المعلومات الحيوية المتعلقة بقوة الأعداء ومواضع الضعف عندهم من العوامل الحاسمة التي تؤدي إلى رجحان كفة أحد الأطراف المتخاصمة في النزاعات السياسية والاقتصادية وفي الحروب العسكرية، وذلك منذ فجر التاريخ، وربما أيضاً قبل بداية التاريخ الجلي.

ولقد بذل البشر أقصى جهودهم من أجل الحصول على هذه المعلومات وما يزالون إلى يومنا الحاضر حيث تستغل الدول والأمم أحدث التقنيات وتستثمر أقصى طاقاتها للحصول على ما يفي بحاجاتها. وهذا السعي ليس محصوراً بالحكومات والجيوش وإنما تعداهم إلى الشركات الخاصة وأيضاً إلى الأفراد العاديين، حيث أن المنافسة باتت تسيطر على جميع مجالات الحياة الإنسانية، وفي ذلك ما يحتم ضرورة الحصول على أكبر قدر ممكن من المعلومات.

ولقد تطورت أساليب التجسس وجمع المعلومات عبر

العصور ولم تعد تقتصر على الجاسوسات الفاتنات اللواتي يقمن بإغواء قادة الاعداء. لقد باتت هذه الأساليب تعتمد إعتماداً كبيراً على التكنولوجيا وبشكل خاص على التكنولوجيا الإلكترونية والمعلوماتية من أجل التنصت على أحاديث واتصالات الأعداء لكشف كل ما تحتويه خزائنهم وحقائبهم من أغراض وأوراق.

لقد بينت التطورات التي حصلت خلال الثمانينات والتسعينات بصورة لا تقبل الشك أهمية هذه الأعمال، حيث أكدت وسائل الاعلام الأميركية بأن الولايات المتحدة قامت بعملياتها العسكرية ضد العراق وليبيا والسودان وأفغانستان بناء على معلومات وردتها على شكل تقارير مستقاة من عمليات للتنصت على الاتصالات الهاتفية، أو لاستراق التجسس على حركة التحويلات المالية الخاصة ببعض الحركات المعادية للولايات المتحدة. كذلك فقد يكون الأمر الأبرز الذي أظهرته أزمة المراقبين الدوليين في العراق أواخر 1998 وأوائل 1999 هو أن هذه الأزمة أظهرت مدى أهمية أعمال التجسس والتنصت على الاتصالات لتحديد معالم السياسة الخارجية الأميركية، حيث اتهمت الحكومة العراقية المراقبين بأنهم زرعوا المراكز الحكومية في العراق بأجهزة التنصت وأرسلوا تقاريرهم إلى وكالات

المخابرات الأميركية بصورة مباشرة بدل حصر تعاونها مع هيئة الأمم المتحدة، وقد عادت صحف أميركية وبريطانية وأكدت هذه المعلومات..

المهم في الموضوع هو أن الولايات المتحدة تركز جهودها على أن تكون مطلعة على كل شاردة وواردة تحصل في العالم ويمكن أن تؤثر على مصالحها، ومن أجل تحقيق هذا الهدف تستعمل ترسانة هائلة من أجهزة التنصت والاقمار الاصطناعية ومراكز معالجة البيانات. ولقد أصر الرئيس الأميركي السابق جورج بوش نفسه على الاشادة بالجهود التي بذلتها وكالة الأمن القومي الأميركي طيلة أعوام ولايته، مع الاشارة إلى أن بوش المذكور عمل رئيساً لوكالة المخابرات المركزية الأميركية سي.آي.أي (CIA) في أواسط السبعينات...

غير أن الولايات المتحدة ليست الوحيدة الناشطة في هذه المجالات، بل أن جميع الحكومات أدركت أهمية الحصول على المعلومات لضمان مصالحها الحيوية، كما أن هذا الادراك لا ينحصر على الدول والحكومات فقط، وإنما يشمل كذلك الشركات الخاصة والأفراد العاديين، وقد باتت تتوفر معدات معقدة تتيح التقاط وتسجيل الأصوات بطريقة متقنة في المتاجر المتخصصة وتطرح بأسعار معقولة بحيث انها شبه متوفرة للجميع...

وتلعب تكنولوجيا المعلومات دوراً أساسياً في معالجة وتحليل البيانات التي يتم التقاطها وذلك بالنظر إلى أن الكمية الهائلة من هذه المعلومات وتعدد فئاتها إلى درجة أنه لا يمكن تعدادها إلا بواسطة أنظمة معلوماتية ذات سرعة فائقة وسعة تخزينية عملاقة لكي يصبح بالامكان الاستفادة منها بصورة مجدية.

وتدور قصص وروايات عديدة حول قيام الأجهزة الأمنية في عدد من الدول الصناعية الغربية، وخصوصاً في الولايات المتحدة بمراقبة المواطنين العاديين من دون علمهم أثناء قيامهم بأبسط أعمال الحياة اليومية مثل سحب النقود من الجيب أو مجرد السير على الأقدام.

والواقع أن الكثير من هذه الروايات مبالغ فيها. إلا أن الحقيقة أيضاً هي أن التكنولوجيا التي تسمح بإجراء أعمال المراقبة بهذا الشكل متوافرة في العديد من الأحيان.

وهذه نبذة حول أبرز ما يجري تداوله بهذا الشأن:

- تتضمن الأوراق النقدية التي أصدرتها الخزينة الأميركية في السنوات الأخيرة شرائح من مادة البوليستر؛ ويقول بعض الناس أن الهدف من وضع هذه الشرائح هو تمكين دوائر الأمن من تحديد عددها بواسطة ماسحات خاصة، وبالتالي معرفة قيمة

الأموال التي يحملها كل شخص في جيبه وكيفية انفاقه إياها، وأيضاً لتعقب هذا الشخص لدى تنقله.

وتؤكد الخزينة الأميركية أن هذه الروايات لا تستند إلى أية حقيقة وإلى أن الأجهزة الماسحة المذكورة غير موجودة....

- يمكن تعقب الاشخاص عن طريق زرع شرائح الكترونية في أجسادهم تبث إشارات كهربائية بصورة مستمرة وتسمح بمراقبة كل تحركاتهم. ويؤكد تيموثي ماك فيغ (Timothy Mc Veigh) المتهم بتفجير مقر إدارة المباحث الأميركية في مدينة أوكلاهوما سيتي في نيسان (ابريل) 1995 أن الدوائر الأميركية زرعت شريحة من هذا النوع في أحد ردفيه.

والأمر الأكيد هو أنه توجد في الأسواق عدة شرائح الالكترونية صغيرة مصممة لتزرع في أجسام الحيوانات الأليفة لكي يصبح بالإمكان إيجادها بسهولة، وأن لا شيء يمنع من زرع هذه الشرائح في جسم الإنسان.

- هناك إشاعة تؤكد بأن وكالة المخابرات المركزية الأميركية «سي آي أي» (CIA) تقوم بمراقبة كل شخص داخل الولايات المتحدة عن طريق الموجات الكهرومغنطيسية حيث يكون لكل شخص إشارة كهرومغنطيسية خاصة تكون الوكالة قد وضعتها سراً. وهذه الاشاعة غير صحيحة على الأرجح.

-كما أن ثمة رواية تؤكد بأن هناك أنظمة كمبيوترية في بلجيكا حيث المقر العام لحلف شمالي الأطلسي «الناتو» تخزن فيها المعلومات حول كل شخص حي على الكرة الأرضية. وقد يكون الصحيح هو أن هناك أنظمة كمبيوترية في بلجيكا تخزن فيها المعلومات حول أشخاص معينين من عدة بلدان يهتم بمراقبتهم حلف شمالي الأطلسي.

وبالنظر إلى أهمية الموضوع ومدى تأثيره على المصير القومي كان لا بد من التطرق إليه بصورة علمية ودراسة تقنيات التجسس المعتمدة حالياً لدى الدول والجيوش ولدى الشركات الخاصة، مع التركيز على النشاط الاستخباراتي الاميركي أولاً، وذلك بالنظر إلى أن الولايات المتحدة هي القوة العظمى الأبرز ومن دون منازع في هذا المجال بالوقت الحاضر وبعد ذلك تقنيات التنصت وأعمال التجسس الاقتصادي والنشاط اليهودي في هذا المجال، وننتهي إلى البحث في مستقبل النشاط المخابراتي، ومدى تأثيرها على المستقبل القومي.

الفصل الأول:

النشاط المخابراتي الأميركي

الخلفية التاريخية: يعتبر العديد من المؤرخين بأن اهتمام الولايات المتحدة بتطوير شبكتها المخابراتية حتى المستوى الذي بلغته اليوم يعود إلى غارة الطائرات اليابانية على قاعدتها البحرية في بيرل هاربور (Pearl Harbor) سنة 1941، والتي كانت السبب في دخول أميركا في الحرب الكونية الثانية.

ولقد حملت هذه الحادثة الحكومة الأميركية على القيام بحملة شاملة لتطوير أنظمة التنصت أدت حينها إلى توظيف نحو 10,000 خبيراً، وسمحت للقوات الأميركية بخرق نظام الاتصالات العسكرية اليابانية والالمانية. وبعد الحرب الثانية ركز الأميركيون جهودهم على التجسس ضد الاتحاد السوفياتي والبلدان الاشتراكية، وأبرموا اتفاقات سرية للتعاون بهذا الصدد مع بريطانيا وكندا وأوستراليا.

وقد تمكن الاميركيون في سنة 1949 من فك شيفرة اتصالات السفارة السوفياتية في واشنطن، وهو ما سمح لهم بالقاء القبض على العلماء النوويين الأميركيين اليهود ذوي الميول اليسارية والصهيونية كلاوس فوشس (Klaus Fuchs) والزوجين روزنبرغ (Rosenberg) الذين كانوا يعملون سراً لحساب السوفيات وقد تمت محاكمتهم بتهمة اقتراف جرم الخيانة العظمى في الخمسينات.

وأبرز وكالات المخابرات الأميركية هي:

● وكالات المخابرات الأميركية:

تعتبر وكالة المخابرات المركزية الأميركية «سي آي أي» (CIA) المتخصصة بجمع المعلومات التي تخص سياسية الخارجية الأميركية ومكتب التحقيقات الاتحادي «أف بي آي» (FBI) المتخصص في جمع المعلومات الخاصة بالأمن الداخلي الأميركي ووكالة الأمن القومي «أن أس آي» (NSA) المتخصصة بأعمال التنصت والرقابة أشهر الوكالات المخابراتية الأميركية، بيد أنها ليست الهيئات الوحيدة العاملة في مجالات جمع وتحليل المعلومات حيث هناك عدة وكالات متخصصة تعمل في معالجة فئات محددة من البيانات.

ويبلغ العدد الاجمالي للوكالات المخابراتية الاميركية 13

وكالة بالوقت الحاضر، مع إمكانية وجود وكالات سرية لم يكشف النقاب عنها وتقوم بأعمال بالغة السرية. ويعمل في مجمل هذه الوكالات نحو 100,000 مواطناً أميركياً وبلغت الميزانية الاجمالية المرصودة لهذه الوكالات في السنة المالية 1998 26,7 بليون دولار أميركي، وهي تقارب الـ 29 بليون دولار في السنة المالية 1999، وكل ذلك حسب ما صرح به مدير وكالة «سي آي أي». وتبلغ ميزانية وكالة «ان اس آي» وحدها، 16 بليون دولار.

ولا بد من الاشارة إلى أنه تحصل في أحيان كثيرة خلافات ونزاعات في ما بين هذه الوكالات، وذلك نتيجة لتضارب الصلاحيات والتنافس على ابراز المنجزات المحققة، وأشهر هذه النزاعات هي تلك القائمة بين وكالة «سي آي أي» ومكتب «أف بي آي».

وتعتبر وكالة الأمن القومي أهم الوكالات المخابراتية الأميركية في الوقت الحاضر والأكثر تأثيراً على مسار السياسة الخارجية الأميركية. وتأسست هذه الوكالة سنة 1952 وكان لها فضل كبير في تطوير تقنيات الاقمار الصناعية لاعمال الرقابة، وكذلك أجهزة التنصت وأنظمة السوبر كمبيوتر، وحتى أشرطة الكاسيت السمعية المعروفة...

ومن الناحية العملية، يمكن القول من دون مبالغة بأن التقارير المخابراتية التي يتلقاها المسؤولون الاميركيون هي التي

تحدد معالم السياسة الخارجية الأميركية، وهناك أكثر من دليل على ذلك، من الشهادة العلنية التي منحها الرئيس الأميركي السابق جورج بوش (George Bush) تقديراً وتثميناً لوكالة الأمن القومي الأميركي «أن أس آي» (National Security Agency,NSA) عند تركه البيت الأبيض سنة 1993، إلى ما تردد من أن مواقف جورج بوش إياه المناهضة للعسكريين السوفيات الذين قاموا بمحاولة انقلابية فاشلة في صيف 1991 كانت نابعة من تقارير وردته من وكالة «ان سي آي» تؤكد على تردد هؤلاء العسكريين وانقسامهم في ما بينهم، وقد تبين ذلك من جراء التنصت على الاتصالات التي اجروها لدى قيامهم بمحاولة الانقلاب، إلى اعتراف مدير وكالة أن أس آي نفسه سنة 1994 بأنه «لا يوجد أي جانب من جوانب السياسة الخارجية الخاصة بحكومة الولايات المتحدة لا تتدخل فيه الوكالة..».

وكان من الطبيعي والمنطقي أن يؤدي هذا النشاط البالغ من قبل الوكالة إلى تبرم وتضايق الدول الأخرى، وليس الدول المناهضة لأميركا فقط وإنما أيضاً البلدان الغربية المتحالفة معها، وقد تجلى هذا التبرم باصدار مجلس نواب الاتحاد الأوروبي في مدينة ستراسبورغ احتجاجاً رسمياً تم توجيهه إلى الحكومة الأميركية، حيث أن البرلمان الأوروبي اعتبر أن نشاطات التنصت

الأميركية تمس سيادة الدول التي تعمل فيها وتخالف أصول الحفاظ على الحياة الخاصة للأفراد، (وذلك في سنة 1998).

ويبدو أن هذه الاحتجاجات لم تؤثر كثيراً على الحكام الأميركيين، حيث ما تزال الحكومة الاميركية ومجلسي الكونغرس تؤمن وكالات المخابرات الأميركية المختلفة بميزانية بالغة، وذلك على الرغم من اتباع سياسات تقشفية، مع السعي إلى توسيع نطاق النشاطات المخابراتية... ووكالة الأمن القومي هي «الابنة المدللة في واشنطن»، إذا جاز التعبير، لكن ما هي بالضبط الأعمال التي تقوم بها هذه الوكالة؟

●أبرز منجزات وكالة الأمن القومي:

وكالة الأمن القومي الأميركي هي أكثر الدوائر المعروفة في الدولة الأميركية سرية من غير منازع، ومن الطبيعي اذ ذاك ان تكون المعلومات الدقيقة حولها نادرة مع الافتقار إلى الدقة والتفاصيل؛ بيد أنه بدأت تصدر كتب وتحقيقات تتناول هذا الموضوع تلقي الأضواء وتكشف الحقائق حوله؛ وغالباً ما تكون هذه الدراسات من تأليف صحافيين وكتاب متخصصين أو من عملاء سابقين عملوا في الوكالة.

بالاستناد إلى هذه المعلومات غير المؤكدة، فإن وكالة «أن أس آي» قادرة على التنصت على ما لا يقل عن 95٪ من جميع

الاتصـالات السلكيـة واللاسلكيـة التي تجـري في العـالم، وتقـوم بمعـالجة كمية من البيانات يوازي حـجمـها كمية البيانات المخزنة في مـجلدات مكتبة الكونغرس الاميركي (وهي أكبر مكتبـة في العالم قاطبة) كل ثلاث ساعات، باعتراف مدير الوكالة نفسه..

وغني عن البيـان بأن الوكـالة لا تقـوم بمعـالجـة جـمـيع الاتصالات التي تستطيع الولوج إليها وإنما تختار من بينها ما تعتبر بأنه يؤثر على المصلحة القومية للولايات المتحدة.

ويعتقد على العموم بأن الوكالة تقوم بمعالجة 10,000 إلى 15,000 اتصالاً هاتفياً كل يوم، في حين تؤكد بعض المصادر بأن عدد الاتصالات التي تتم معالجتها يصل إلى عشرات الألوف من الاتصالات.. ومن الطبيعي أن يكون هذا العدد من أكثر الأسرار الاميركية حساسية..

ولا يقتصر نشاط وكالة «أن أس آي» على مراقبة المخابرات الهاتفية بل انه يشمل كذلك الاتصالات اللاسلكية، وبدأ يغطي أيضاً الاتصالات التي تتم عبر شبكة الانترنت.

وتؤكـد مـصـادر عـديدة بأن نشـاط وكـالة «أن أس آي» لا يقتصر أبداً على البيانات التي تهم السياسة الخارجية الأميركية، بل تشمل أيضاً ما يهم الشركات الأميركية الرئيسية، وفي هذا المجال أكدت بعض الأوساط العليمة أن مجموعة جنرال موتورز

(General Motors) لصناعة السيارات تمكنت من الحصول على اثباتات تؤكد ضلوع شركة فولكزفاغن (Volkswagen) في عملية تجسس صناعي استهدف فروعها الأوروبية (أي الفروع الأوروبية لجنرال موتورز) بفضل تقارير وردتها من الوكالة. بيد أن وكالة الأمن القومي ليست الوحيدة التي تزود الادارة الاميركية بالمعلومات، كما سبق وأن اشرنا إليه. والواقع أن كثرة مصادر المعلومات باتت تشكل عائقاً للأميركيين أكثر مما هي مكسباً لهم، ولذلك أرتأى المسؤولون إنشاء شبكة كمبيوترية متخصصة في توزيع المعلومات على جميع المعنيين بها على طريقة شبكة الانترنت. وتعود فكرة انشاء هذه الشبكة إلى أنه خلال حرب الكويت، اشتكى بعض القادة العسكريين الاميركيين من أنهم لا يتلقون البيانات المخابراتية الخاصة بالوضع الميداني على الجبهة بالسرعة الكافية. وذلك بسبب بطء اجراء اعمال الفرز والمعالجة والتوزيع.

وحدا هذا الأمر القيادة العسكرية الاميركية إلى انشاء شبكة بيانية خاصة بها هي شبكة انتلينك (Intelink) سنة 1994، وذلك لتوزيع البيانات المخابراتية على جميع المعنيين بها بصورة آنية.

وشبكة انتلينك هي نوع من شبكة انترنت خاصة بوكالات المخابرات الاميركية يتم فيها توزيع المعلومات السرية التي

حصلت عليها كل وكالة، وبذلك تكون هذه المعلومات مشتركة، وليست محصورة في وكالة دون غيرها كما كان الأمر عليه في السابق. (ونذكر هنا على الهامش بأن شبكة الانترنت صممت أساساً سنة 1969 لتشكل شبكة عسكرية أميركية رديفة لتأمين الاتصالات في حال نشوب نزاع نووي يسفر عن تدمير شبكات الاتصالات المعتمدة؛ وقد تحولت في ما بعد إلى الشبكة المدنية التي نعرفها اليوم ويمكن القول أن انتلينك تمثل نوعاً من العودة إلى الينابيع الاصلية للانترنت). ويمثل هذا التوجه تحولاً جذرياً في الفلسفة السائدة لدى أوساط المخابرات الأميركية، وسبب هذا التحول هو أن المسؤولين ارتأوا بأن حصر معلومات معينة في وكالة دون غيرها يقلل من الفائدة التي يمكن جنيها من هذه المعلومات، فضلاً عن أن هذا الواقع يخلق حالات تنافس ونزاعات بين الوكالات المخابراتية المختلفة...

ومن الناحية التقنية، فان انتلينك تتألف من 100 موقعاً متخصصاً تقريباً، (ذلك في أول سنة 1999 حسب المعلومات المتوفرة) ويعتمد تشغيلها على برامج كمبيوترية مدنية عادية خاصة بشبكة الانترنت، وأبرز هذه البرامج هي برنامج التصفح من شركة نتسكايب (Netscape) وبرنامج البحث عن البيانات التافيستا (Altavista). وتتضمن هذه المواقع 440,000 صفحة

الكترونية (في حين أن عدد الصفحات الالكترونية الخاصة بصحيفة واشنطن بوست Washington Post لا تزيد عن 24,000 صفحة الكترونية، علماً أن واشنطن بوست هي إحدى أهم الصحف الأميركية). ويشترك في تسهيلات شبكة انتلينك نحو 50,000 شخصاً يتوزعون بين محللين للبيانات وضباط عسكريين ورجال سياسة.(وهذه الأرقام خاصة بأوائل 1999).

ومن الناحية الامنية، شددت وزارة الدفاع الأميركية على «تصفيح» الشبكة لكي يستحيل على القراصنة التسرب إليها، ويمكن تلخيص الاجراءات الامنية التي تم اتخاذها بالآتية:

- ليس لشبكة انتلينك أي اتصال بشبكة الانترنت.

- على جميع من يريد الاشتراك في هذه الشبكة الحصول على ترخيص أمني خاص وبالغ السرية.

- إن جميع الطرفيات التي يمكن بواسطتها الاطلاع على بيانات شبكة انتلينك موجودة في مبانٍ حكومية تحت حماية وزارة الدفاع الأميركية.

- لقد تم تشفير البيانات التي يتم تداولها في الشبكة بواسطة خوارزمية معقدة طورتها وكالة الأمن القومي الأميركية. بيد أن الخطر على خرق سرية الشبكة (الخطر هنا هو من وجهة النظر الأميركية، في حين أن هذا الخطر يشكل فرصة جيدة سعيدة

لاعداء أميركا بطبيعة الحال...) هو داخلي أكثر مما هو من قراصنة خارجيين، بمعنى أن أحد المشتركين على الشبكة قد يعمد إلى تحويل البيانات السرية التي يطلع عليها إلى جهة معادية للولايات المتحدة. ويرد أنصار انتلينك على هذا الاحتمال بالقول أن المعلومات البالغة السرية تبقى محصورة بالمعنيين بها، وأن لكل وكالة مخابراتية أميركية شبكتها الكمبيوترية الخاصة (أي شبكة «انترانت») معزولة عن شبكة انتلينك بواسطة برامج «جدران النار»(Firewall Software).

خلاصة القول أن انتلينك تشكل تبديلاً تقنياً هاماً في شبكات المخابرات الأميركية إلا أنه لا يمثل بالضرورة ثورة جذرية في ادراك معاني مفهوم العمل المخابراتي والتجسسي كما أن هذه الشبكة لم تقضِ على أسباب مشاكل الاستخبارات الاميركية، من مخاطر تسريب المعلومات إلى التنافس بين الوكالات فضلاً عن المشكلة الأبرز التي تعاني منها المخابرات وتتمثل بتكاثر المعلومات المجموعة من مصادر متعددة إلى درجة يستحيل معها فرزها وتحليلها ومعالجتها بطريقة مجدية...

وأخيراً، لا بد من الاشارة إلى أن زبيغنيو بريزنسكي (Zbigniew Brezinski) الذي عمل مستشاراً للرئيس كارتر (Carter) لشؤون الأمن القومي اعترف في حديث صحافي أدلى

به إلى المجلة الفرنسية لو نوفيل أوبسيرفاتور (Le Nouvel Observateur) بأن الولايات المتحدة لا تكتفي بممارسة اعمال التجسس ضد خصومها وإنما تشمل حلفاءها أيضا بهذه «النعمة».

ملحق

بعض الأمثلة حول الطبيعة السرية المطبقة لهيئات المخابرات الأميركية

ـ تأسس مكتب ان أر أو سنة 1961 ولم تعترف الحكومة الأميركية بوجوده سوى سنة 1992.

ـ تبين أن المسؤولين عن مكتب أن أر أو كانوا يجهلون وجود ميزانية خاصة بمكتبهم بقيمة عدة ملايين من الدولارات خصصت للقيام بأعمال سرية، خارج الولايات المتحدة، وهو الأمر الذي حال دون صرف هذه الميزانية...

ـ أبقى «لوغو» مكتب ان أر أو سرياً حتى 1992.

ـ استعملت «التقنيات الخفية» (Furtive technologies) لبناء مقر ان اراو ذلك لامتصاص موجات الرادار ولكي يصعب اكتشافه ورصده من قبل جهات معادية للولايات المتحدة.

ـ يقال ان المعنى الحقيقي لأحرف «أن أس آي» ليس وكالة الأمن القومي (National Security Agency) وإنما «لا تقول شيئاً أبداً» (Never Say Anything).

ـ يمنع على العاملين لدى أن أس آي السفر إلى خارج الولايات المتحدة في العادة.

ـ هناك حياة اجتماعية منظمة جيداً في وكالة «أن أس آي» مع وجود قاعات للسينما ومسارح ومطاعم وغير ذلك، والهدف هو شد أواصر الألفة في ما بين العاملين والعاملات مع تشجيعهم على أن يتزوجوا في ما بينهم.

ـ تؤمن وكالة «أن أس آي» الجراحين وأطباء الأسنان إلى العاملين لديها للحؤول دون أن يتكلموا أمام غرباء عندما يتم تخديرهم لاجراء عمليات جراحية.

ـ عقدت وكالة «أن أس آي» اتفاقات للتعاون مع معظم بلدان الكومنولث البريطاني ويتوجب على رؤساء حكومات هذه البلدان أن يقسموا بعدم كشف بنود هذه الاتفاقات.

ـ تعمل وكالات المخابرات الاميركية على توظيف علماء للرياضيات وخبراء للكمبيوتر من مواطني بلدان أجنبية (أي غير الولايات المتحدة) ويختارونهم اجمالاً بين الطلبة الأجانب في الجامعات الأميركية، ويتم اغراءهم مع الرواتب المرتفعة (على الأقل بالمقارنة مع الرواتب التي تؤمنها البلدان الأصلية لهؤلاء العلماء) وتسهيل حياتهم في أميركا. ويعود السبب في ذلك إلى تدني المستوى الثقافي الأميركي بصورة عامة، وفق ما جاء في

العديد من التقارير الصادرة في أميركا نفسها. إلا أن ما يحصل بعد توظيف هؤلاء هو أنه يتم منعهم من زيارة أوطانهم الأصلية، وإذا حصل وان سُمح لهم بالقيام بزيارة قصيرة إلى الأهل هناك، فإن عميلاً من المخابرات الأميركية يرافق العامل الأجنبي في سفره من أجل مراقبته ومنع انفلاته من قبضة الحكم الأميركي، كما تُفرض عليه الاقامة في الفندق، بجوار العميل المراقب (بكسر القاف) وليس في بيته العائلي... وهناك عدة أمثلة لذلك وقد عاشتها عدة عائلات عربية بصورة خاصة.

الفصل الثاني:

تطوير مفهوم الأمن القومي الأميركي ودور المخابرات فيه

تحدد الولايات المتحدة الأميركية الخطوط العريضة لسياستها الخارجية بما يتناسب مع «أمنها القومي» (National Security)، ودور الأمن القومي الأميركي هو حماية المصالح الحيوية للولايات المتحدة من سياسية وأمنية واقتصادية وغيرها.

ولقد تم في 1947 سن قانون الأمن القومي الأميركي، مع تشكيل مجلس الأمن القومي (National Security Council) المولج بتقديم المشورة للرئيس الأميركي في ما يتعلق بتنسيق السياسات الأميركية الخارجية والداخلية والعسكرية وضمان التعاون والتنسيق في ما بين الوزارات والادارات الأميركية في المواضيع المتعلقة بالأمن القومي (الأميركي).

ويتولى الرئيس الأميركي تعيين العاملين في هذا المجلس وقد تزايد نفوذه مع السنوات إلى درجة أنه بات

أكثر أهمية من وزارة الخارجية عند رسم السياسات الخارجية، مع العلم بأن اليهودي هنري كيسنجر (Henry Kissinger) كان مديراً لهذا المجلس قبل تعيينه وزيراً للخارجية... مع الاشارة هنا إلى أن اللوبي اليهودي الأميركي تمكن من فرض هيمنته على هذا المجلس.

ويعتمد مجلس الأمن القومي اعتماداً مكثفاً على الأعمال الاستخباراتية للحصول على المعلومات التي تتيح له اعداد تقاريره، وسوف يتزايد هذا الاعتماد في السنوات المقبلة، كما ينتظر بأن يتعزز الاستقطاب في تحديد مفهوم الأمن القومي الأميركي، مع ادما ج جميع الوكالات الأمنية والمخابراتية ضمن وكالة واحدة.

ولقد صدرت عدة دراسات تدعو إلى الأخذ بهذه النظرية، وينتظر أن يؤخذ بالآراء المستعرضة في هذه الدراسات في غضون السنوات القليلة المقبلة.

ومن الأمثلة النموذجية دراسة صدرت في 1998 وأعدها مركز الدراسات الاستراتيجية والدولية «سي أس آي أس» (Center For Strategic and International Studies, CSIS) حول تطور الأمن القومي الأميركي على ضوء ظهور تقنيات جديدة لجمع المعلومات ومعالجتها واستغلالها.

اقترح المركز ادماج الأدوار الأمنية الموزعة حالياً بين عدة وكالات حكومية أميركية في وكالة موحدة للأمن

القومي، بحيث تتولى هذه الوكالة اعداد تقارير بالاستناد إلى المعلومات الواردة من مصادر متعددة، مع جمعها بطريقة متجانسة وموحدة، بحيث يتسنى للرئيس الأميركي اتخاذ القرارات المناسبة على ضوئها على نحو أسرع وأكثر دقة.

وأكد تقرير صادر عن المركز بأن تكنولوجيا المعلوماتية تتيح إقامة علاقة وثيقة بين وزارتي الدفاع والخارجية وبين وكالات المخابرات، بحيث لا يعود هناك مجال للفصل بين الدفاع والدبلوماسية والمخابرات والتكنولوجيا.من أبرز التكنولوجيات الجديدة التي تتحقق هذه النظرية بواسطتها:

- تغيير أساليب الحرب مع تكنولوجيات جديدة للاستشعار وللتصويب.

- ادماج تقنيتي الكمبيوتر والتلفزيون.

- التقدم الذي طرأ على صناعة الشرائح الالكترونية (Microchips) حيث ينتظر بأن تحتوي شريحة الكترونية بمفردها على بليون ترانزستور بحلول العام 2010.

من ناحية موازية، قدرت وزارة التجارة الأميركية بأن تكنولوجيات المعلومات أتاحت أمام الاقتصاد الأميركي تحقيق توفير في التكاليف مقداره 25٪ بين 1993 و1998.

- لقد أتاحت التكنولوجيا الجديدة صنع معدات مثل

أجهزة كاميرات صغيرة، أو أنظمة للواقع الظاهري (Virtual Reality Systems) وأسلاك بصرية للاتصالات تحت البحار، أو انتاج برامج للأعمال الجماعية، وأدى كل هذا إلى ظهور أنماط جديدة من الأعمال المالية والتجارية.

خلاصة القول أن تقنيات المخابرات لم تعد مجرداداة لتنفيذ سياسات الأمم، وإنما عاملاً أساسياً في تحديد معالم هذه السياسات، وهذا الاستنتاج لا يختص بالسياسات الأميركية فقط، وإنما بسياسات جميع الدول المتقدمة اقتصادياً وتكنولوجياً.

الفصل الثالث:

أنظمة الرقابة والتجسس بواسطة الأقمار الاصطناعية

تعتمد الدول الكبرى، وعلى رأسها الولايات المتحدة، إعتماداً كبيراً على الأقمار الإصطناعية للقيام بأعمال المراقبة والتنصت على الدول الأخرى، وذلك منذ الستينات حيث كانت الأزمة الرئيسية في العالم هي ما عرف بالحرب الباردة بين الدول الغربية من جهة ودول المعسكر الاشتراكي من جهة ثانية.

أيام الحرب الباردة كانت الاقمار الإصطناعية تقوم بأعمال «الدورية» فوق منطقة معينة مرتين أو ثلاث مرات كل 24 ساعة، وهذا ما يكفي للافادة عن تحركات جوية أو برية أو بحرية مشبوهة.

ولقد تغيرت أولويات الدول الغربية بعد نشوب حرب الكويت، حيث أيقن المسؤولون العسكريون بأن الحصول على

صورتين أو ثلاث صور لميدان المعركة لم يكن كافياً، وأن المطلوب هو إجراء أعمال مراقبة مستمرة ومتواصلة.

ولدى الولايات المتحدة 50 محطة تنصت (على الأقل) موزعة بين عشرين بلداًفي القارات الخمس، وأهم هذه المحطات كائنة في بريطانيا وزيلاندا الجديدة واليابان والمانيا وأوستراليا، فضلاً عن الولايات المتحدة بطبيعة الحال...

وتقوم هذه المحطات بالتقاط البيانات التي يتم تبادلها بواسطة الاقمار الاصطناعية عند نقل هذه البيانات من القمر الاصطناعي إلى الكرة الأرضية.

كما أن لدى الوكالة أقمار أخرى مخصصة لها يتم اطلاقها ووضعها في مدارات قريبة من مدارات أقمار الاتصالات، وهذه الأقمار الخاصة تلتقط البيانات التي تستقبلها أقمار الاتصالات وتعيدها إلى محطة الوكالة.

وهذه الأقمار التجسسية مصنوعة بتقنية بالغة السرية، وهي مزودة بهوائيات توازي مساحتها مساحة ملعب لكرة القدم، وهي قادرة أيضاً على استراق الاتصالات التي تتم بواسطة أجهزة الهاتف الخلوي. وهناك 9 أقمار من هذا النوع على الأقل وفق المصادر العليمة.

وهناك هيئة سرية أميركية متخصصة في التصوير

الفضائي بواسطة الأقمار الاصطناعية، ولقد تم انشاء هذه الهيئة سنة 1961؛ هذه الهيئة هي «المكتب القومي للاستكشاف «ان ار أو» (National Reconnaissance Office, NRO) وهي متخصصة في التصوير وتصل نسبة وضوح الصور التي[2] تلتقطها إلى حد أنه يمكن تعيين أشياء لا يزيد حجمها عن 10سم من على بعد مئات الكيلومترات .يعني هذا من الناحية العملية بأنه يمكن تميز نوع السيارات في صورة ملتقطة من الفضاء.

وهناك أقمار اصطناعية أخرى تعمل بتقنية الرادار، وهي قادرة على التصوير عبر السحاب وفي الليل.

وكما أنه تستعمل أقمار اصطناعية حرارية مزودة بنظام التقاط يعمل بالأشعة ما دون الحمراء وتستطيع تبين حصول أي تبديل في درجة الحرارة في أرض المنطقة التي تتم تغطيتها، حتى اذا كانت هذه التبديلات تبلغ عُشر (10٪) من الدرجة المئوية، وتستعمل الاقمار الاصطناعية بصورة خاصة لمراقبة النشاطات التي تتم تحت مستوى الأرض، من قبيل المصانع السرية للأسلحة وغيرها.

وتؤكد مصادر فرنسية عليمة أنه تم اطلاق نحو 15 قمراً اصطناعياً مزوداً بجميع هذه القدرات في المدة الأخيرة وتعرف بأقمار ك ايتش 12 امبيروفيد كريستال (KH 12 Improved

.(Crystal

على أن هذا هو من قبيل الترجيحات والتقديرات، ولا يمكن الجزم بمدى صحة ودقة هذه المعلومات؛ ومن المعلومات الأكيدة أن الاقمار التجسسية المستقبلية (وعلى الأرجح العديد من الأقمار الحالية أيضاً) سوف تعتمد على تقنية شبيهة بتلك المستعملة في الأقمار الاصطناعية التصويرية المدنية مثل القمر الفرنسي سبوت (SPOT) أو القمر الأميركي لاندسات (Landsat)، مع الاشارة إلى أن نوعية ودقة الصور التي ترسلها هذه الأقمار هي أفضل من صور بعض الأقمار الإصطناعية العسكرية.

وهناك نوعان رئيسيان من الأقمار الأميركية للتصوير: أقمار كيهول (Keyhole) التي تلتقط صوراً من النوع الفوتوغرافي وأقمار لاكروس (Lacrosse) التي تستعمل تقنية التصوير الراداري.

وتقول بعض المصادر بأن كلفة قمر كيهول تبلغ نحو بليوني دولار. وتستطيع هذه الأقمار إلتقاط صور عن الأرض لا تتجاوز قياساتها 15 سم أي ما يكفي للتمييز بين شاحنة ودبابة.

ويرجح أن أقمار لاكروس تستعمل تقنية التصوير المعروفة بـ«رادار الفتحة التركيبية» (Synthetic Aperture Radar)، وتبث موجات صغرية باتجاه الأرض ثم تلتقط انعكاساتها المرتدة إلى

القمر. ويمكن تحليل هذه الصور الرادارية بواسطة برامج كمبيوترية خاصة لتحويلها إلى صور مفهومة. والميزة الرئيسية لهذه التقنية هي أنها تسمح بتخطي الغيوم والأمطار والغبار، وإنها تصلح للاستعمال أثناء الليل، حيث لا تصلح أقمار كيهول.

إلا أن القمرين غير قادرين على ضمان تغطية متواصلة، وذلك بالنظر إلى أن مدارهما منخفض (يبلغ ارتفاع هذا المدار 200 إلى 300 كلم) وسرعتهما مرتفعة. وهذا يعني أن مدة تغطية كل منطقة لا تزيد على نحو دقائق، مع العلم بأن كل قمر من هذه الأقمار يقوم بثلاث دورات حول الأرض كل 24 ساعة.

ويفكر المكتب الوطني الأميركي للاستكشاف باستعمال أقمار اصطناعية ذات مدار مرتفع يتراوح بين 350 كلم في نقطته الأقرب إلى الأرض و5000 كلم في نقطته الأبعد، بحيث يسمح ذلك بمراقبة منطقة معينة لـ 50 دقيقة عندما يكون المدار في نقطته الأبعد، مع إمكانية إجراء 5 عمليات استطلاع وفق هذه المواصفات على أربع وعشرين ساعة. وبذلك يستطيع التقاط صور فيديوية لأرض المعركة، ولو إن هذه الامكانية غير مفيدة جداً بالنظر إلى كلفتها الباهظة. إلا أن الصور الملتقطة من ارتفاعات عالية ستكون ذات نسبة وضوح أقل مقارنة مع تلك الخاصة بالأقمار ذات الارتفاعات المنخفضة وعلى كل حال فإنها تكفي لتمييز الدبابات

وغيرها من المركبات.

وجميع هذه الأقمار الاصطناعية باهظة التكاليف و خسارة قمر واحد يمكن أن يؤدي إلى نقص خطير في المعلومات.

والخسارة هذه يمكن أن تكون نتيجة عملية إطلاق فاشلة، وأيضاً بسبب التعرض لطلقات أسلحة مضادة للأقمار الاصطناعية في المستقبل. ولقد أجرى سلاح الجو الأميركي تجارب على أسلحة من هذا النوع في الثمانينات، وتمكن من اسقاط قمر اصطناعي قديم بواسطتها. ونذكر أيضاً بأن العراق جرب سلاحاً من هذا النوع خلال حرب الخليج، وكان هذا السلاح العراقي كناية عن عدة صواريخ من نوع سكاد (SCUD).

وقد يكمن حل هذه المعضلة الحالية بالاعتماد على عدة أقمار اصطناعية صغيرة وإقتصادية بدل الاعتماد على عدد محدود من الأقمار المعقدة والباهظة التكاليف، مع امكانية صنعها بسرعة، في حين أن عملية صنع قمر تجسس تقليدي تستغرق سبع إلى ثماني سنوات.. ولقد ذكر بأن سلاح الجو الأميركي يدرس إمكانية استعمال أقمار صغيرة في المستقبل.

بيد أن اسقاط الأقمار يمكن أن يتسبب بمضاعفات سياسية وديبلوماسية بالغة، وذلك بالنظر إلى أن العديد من الأقمار الاصطناعية التجارية تملكها بلدان قد تكون حيادية في نزاع

ينشب بين الدولة التي تستفيد من خدمات القمر (اتصالات، صور استكشافية الخ...) والدولة المناهضة لها والقادرة على اسقاط هذا القمر الاصطناعي (وخصوصاً الولايات المتحدة وروسيا)، وبالتالي فان اسقاط القمر لا بد وأن يصنف كعمل عدائي يستهدف البلد الحيادي.

وينتظر أن تزداد حدة هذا التشابك في السنوات المقبلة، مع العلم بأن وزارة الدفاع الاميركية تعتبر بأن 70% من الاتصالات العسكرية سوف تتم بواسطة أقمار تجارية بحلول نهاية العقد الأول من القرن الحادي والعشرين، وقد يتجاوز عدد الاقمار الاصطناعية التجارية الالف قمر في هذا الوقت.

ويدرس الأميركيون تقنيات جديدة «لتحييد» الأقمار غير التابعة لها من دون القيام بعملية عسكرية عدوانية، ومن بين الافكار المطروحة بهذا الصدد:

– اطلاق «طائرة فضائية» تستطيع ابطال عمل الاقمار عن طريق تشويش الموجات اللاسلكية المنبعثة عنها والموجهة إلى الدولة المعادية للولايات المتحدة، أو حجب الاشعاعات الشمسية عن هوائيات القمر الاصطناعي، وهو ما يتسبب بقطع التيار الكهربائي بالطاقة الشمسية وبالتالي بوقفه عن العمل.

- حجز جميع قنوات الاتصالات التي توفرها الاقمار

الاميركية لأطراف خارجية في وقت الأزمات والحؤول دون امكانية أن تستعملها الأطراف المعادية لأميركا.

ـ حجز قنوات الاتصالات في الاقمار غير الأميركية بقدر المستطاع ومع اعتماد الأساليب الترغيب والترهيب لحمل شركات هذه الاقمار على الموافقة. وما يزال هذا النوع من الحروب جديداً كلياً وينتظر أن تتبلور أساليب جديدة في المستقبل غير البعيد.

من ناحية أخرى، تدرس بعض أوساط وكالة الفضاء الأميركية فكرة الاستغناء جزئياً عن الأقمار الاصطناعية واستبدالها بأخذ رائد فضاء عسكري أميركي يقوم بأعمال التصوير بواسطة كاميرا خاصة ذات نسبة وضوح مرتفعة من على متن المكوك الفضائي، إلا أن السؤال هنا يتمحور حول مدى إمكانية استعمال المكوك الفضائي بمرونة كافية لضمان فعاليته أثناء فترات الأزمات والحروب.

هذا ويفكر بعض الخبراء العسكريين الأميركيين بإعتماد وسائل جديدة في حروب القرن الحادي والعشرين. وفي هذا الاطار صدر عن سلاح الجو الأميركي سنة 1993 دراسة عنوانها «سبايسكاست 2020» (Spacecast 2020) تقترح اعتماد تقنيات تتيح للقمر الإصطناعي التجسس على الأطراف المتحاربة والتمييز بين العدو والصديق.

وعملية التمييز هذه تتم عن طريق اطلاق شعاع ليزري موجه إلى المعركة، على أن يكون هذا القمر مزوداً بمجسمات ومستشعرات تسمح بالتمييز بين الإشعاعات المرتدة وذلك عن طريق مقارنة هذه الانعكاسات مع البيانات المخزنة في قاعدة بيانات خاصة بحيث يمكن مثلاً التمييز بين انعكاسات نوع معين من الطلاء الخاص بالدبابات، أو بأسلحة حقيقية أو بأسلحة دبابات مصنوعة من المطاط مثلاً لخداع الأعداء... وغير ذلك...

كما تجري أبحاث أخرى لتطوير نظام لكشف إشعاعات الأسلحة البيولوجية بواسطة الأشعة ما فوق البنفسجية.

مراقبة الاقمار الاصطناعية: وإذا كانت الأقمار الاصطناعية تعتبر الاداة الأبرز للقيام بأعمال المراقبة والتجسس العسكرية فهي أيضاً عرضة لأعمال المراقبة والتعقب ويُعتقد أن الولايات المتحدة تملك 25 قاعدة موزعة في جميع أنحاء العالم لتعقب الأقمار الاصطناعية، ويُزود كل من هذه المواقع بثلاث تلسكوبات عاكسة تتضمن مرايا يبلغ عرضها 40 بوصة وتعطي صوراً لجميع الأشياء الواقعة في مدار فضائي. ويقول سلاح الجو الأميركي بأن لهذه التلسكوبات قدرة على كشف الأشياء المحلقة تفوق قدرة العين البشرية بـ 10,000 ضعف، وانها تستطيع تعقب كرة للعبة في كرة السلة من على مسافة 20,000 ميلاً. وتتحرك

التلسكوبات بطريقة مدارية، وهي مرتبطة بأربعة أجهزة كمبيوتر تتولى تحليل الصور الواردة من كاميرات التلسكوب وتحليلها لفرز كل ما هو غير طبيعي، والمقصود بالطبيعي هو النجوم والكواكب في الفضاء، أما غير الطبيعي فهو أقمار التجسس والاجرام الفضائية.

وبدأت الولايات المتحدة مؤخراً استعمال جهاز تلسكوب بقياس 3,67 م يعرف بالنظام المتقدم الكهروبصري (Advanced Electro- Optical system) وأكدت أن هذا النظام يحسن نسبة الوضوح بالمقارنة مع أجهزة التلسكوب من الأجيال السابقة بنسبة 300٪، وتم تشغيل التلسكوب في قاعدة المراقبة الأميركية في ولاية هاواي، مع قرب اعتمادها في القواعد الأخرى في وقت لاحق..

بيد أن الأقمار الاصطناعية لا تستعمل للأعمال العسكرية والمخابراتية فقط، وإنما أيضاً للاستعمالات الافرادية، وأفضل مثال على ذلك هو نظام جي بي اس لتحديد المواقع.

نظام جي بي اس لتحديد المواقع: بدأ نظام جي بي أس (GPS) لتحديد المواقع يأخذ طريقه للانتشار السريع، إذ باتت عدة شركات تطرحه كتجهيز إضافي بناء على طلب لسياراتها الفخمة، كما يستعمل في عدة تطبيقات أخرى.

والمعروف أن هذا النظام يعتمد على أقمار اصطناعية تدور في مدارات فضائية ثابتة مرتبطة بمحطات أرضية، وبهوائيات الأشخاص المشتركين فيها من أجل تحديد مواقع هؤلاء الأشخاص، ومساعدتهم على إيجاد طريقهم.

ويُعتمد هذا النظام بصورةٍ مكثفة لتحديد ملاحة السفن أو جهة توجه السيارات ويعتمد نظام جي بي اس على أقمار اصطناعية أميركية (أقمار نافستار Navstar)، تم خفض نسبة دقتها في تحديد المواقع إلى 300م.،وذلك بناء على طلب السلطات العسكرية الأميركية التي تخشى بأن يعمد أعداء الولايات المتحدة إلى الاستعانة بهذه الشبكة؛ بيد أن العسكريين الأميركيين مزودين بأنظمة استقبال لاشارات جي بي اس تسمح لهم بالحصول على نسبة من الدقة تبلغ أمتاراً معدودة؛ من ناحية ثانية، فلقد بدأت تطرح في الأسواق الاستهلاكية أنظمة تسمح للأفراد بتحسين نسبة دقة جي بي أس إلى أمتار معدودة أيضاً.

وتلعب أقمار نظام جي بي أس دوراً بالغ الأهمية لتحديد مسارات الملاحة الجوية.

إلا أن هذه الأقمار هي أقمار عسكرية أميركية في النهاية، وتعتمدها الولايات المتحدة في عملياتها العسكرية:

الدليل على ذلك هو أنه عندما يكون الجيش الأميركي يجري

عملية في مكان ما من الكرة الأرضية، يفرض الجيش الأميركي بأن تكون جميع أقمار جي بي أس التي تغطي منطقة العمليات في وضع التشغيل.

من ناحية ثانية، فان الاشارات الخاصة بأقمار جي بي أس معرضة للتشويش، وقد تمكن البريطانيون في 1993 من تشويش هذه الاشارات بواسطة جهاز لبث الموجات الكهرومغناطيسية لم تتعدّ قوته وات واحد وهذا يعني أنه يمكن اللجوء إلى هذا الأسلوب للتسبب بضياع المركبات المرتبطة بشبكة جي بي أس من طائرات وشاحنات وغيرها، وخاصة المركبات المدنية التي لا تكون هوائياتها مصفحة من الناحية المبدئية.

كما لا بد أخيراً من الاشارة إلى أنه يمكن استعمال شبكة جي بي أس لتعقب أثر المشتركين فيها عن طريق تركيب أجهزة لاسلكية صغيرة لا يمكن كشفها في اغراض خاصة بالشخص المطلوب تعقبه، وهذه الأغراض يمكن أن تكون ساعة يد أو اسوارة أو أي شيء آخر، والأجهزة اللاسلكية تتصل بأقمار جي بي اس ثم تحدد الموقع وترسله إلى الجهة التي تتولى مراقبة من يتم تعقب حركاته ...

ملحق

قمر استكشافي راداري أميركي للاستعمالات المدنية والعسكرية

نقدم في ما يلي خبراً حول مشروع أميركي لاطلاق قمر اصطناعي استكشافي يعتمد على التقنية الرادارية في الولايات المتحدة ويستعمل للتطبيقات المدنية والعسكرية معاً، ويبين العلاقة الوثيقة بين التقنيات المدنية والعسكرية في مجال المخابرات، مع سعي دوائر الأمن الأميركية إلى مراقبة جميع النشاطات في هذا المجال.

ينتظر أن تقوم الشركة الأميركية اردي ال سبايس (RDL Space Corp) باطلاق القمر الاصطناعي رادار 1 (Radar 1) سنة 2001. ويتميز هذا القمر الاصطناعي بأنه القمر الصناعي الراداري الأول الذي يتم اطلاقه ليستعمل بتطبيقات مدنية، وهو سيؤمن صوراً رادارية مع نسبة وضوح تصل دقتها إلى متر واحد.

يعتمد القمر (رادار - 1) على رادار ذي فتحة مركية (Synthetic aperture radar) وميزة هذه الرادار أنه يسمح بالتقاط الصور خلال الليل أو النهار وفي كل الظروف المناخية، على عكس الصور البصرية في الأقمار الصناعية التصويرية التقليدية.

تعتزم شركة أو دي ال تركيز جهودها التسويقية لبيع الصور الرادارية على الحكومات ودوائر الدولة، وبصورة خاصة على دوائر المخابرات والاستطلاع التابعة للقوات المسلحة النظامية. وتقول مصادر

اردي ال سبايس أن الشركة التي تستثمر القمر الصناعي التصويري الفرنسي سبوت (Spot) تحقق 65٪ من مبيعات الصور التي يلتقطها سبوت مع الدوائر الحكومية والعسكرية الأميركية، مع العلم أن هذه الصور بصرية وليست رادارية.

تعود موافقة الدوائر العسكرية الأميركية على منح الترخيص للمباشرة باطلاق قمر اصطناعي راداري مدني إلى الرغبة في توفير أموال ميزانية الدفاع، مع التطلع إلى الاستفادة من التطورات التكنولوجية التي تتحقق في القطاع الخاص، بيد أن استثمار القمر الصناعي (رادار - 1) سيخضع لرقابة الدولة الأميركية، إذ أنه سينبغي على شركة اردي ال سبايس الحصول على اذن خاص من الحكومة الأميركية قبل بيع صورة رادارية بنسبة وضوح تصل إلى خمسة أمتار وما دون إلى عميل من القطاع الخاص.

يذكر أن أردي ال سبايس تابعة لمختبرات الابحاث والتطوير (Research & Development laboratoires) وهي متخصصة في تطوير التطبيقات الرادارية للفضاء، وقد عملت لحساب سلاح الجو الأميركي وسلاح البحر الأميركي ووكالة الفضاء «ناسا» (NASA) وقيادة الفضاء الأميركية (US Space Command)، وهذا يعني أن القمر الجديد ليس غريباً عن نشاط الدوائر العسكرية والمخابرتية الأميركية، رغم أنه قمر اصطناعي مدني وليس عسكرياً من الناحية المبدئية على الأقل...

الفصل الرابع:

أعمال التنصت على الاتصالات

يمكن القول أن أعمال التنصت على الاتصالات الهاتفية تعود تقريباً إلى الوقت الذي تمت فيه إقامة أولى الشبكات الهاتفية؛ وكانت تقنية التنصت بسيطة وخالية من التعقيد في البداية، حيث كانت الجهة المتنصِتة (بكسر الصاد) تقوم بتوصيل سلك على الخط الخاص بالجهة المُتنصَت (بفتح الصاد)، عليها، فيتم التقاط جميع ما يجري من اتصالات على هذا الخط...

وما تزال هذه الطريقة معتمدة إلى يومنا الحاضر، إلا أنها لم تعد الوحيدة المستعملة بالنظر إلى تعدد أنواع الاتصالات الهاتفية، من اتصالات تتم بواسطة الاقمار الاصطناعية إلى اتصالات تتم باعتماد التقنية الرقمية إلى اتصالات خليوية إلى اتصالات تتم عبر شبكة الانترنت..

ويتم التنصت على الاتصالات بواسطة الأقمار الاصطناعية بالوسيلة المستعرضة في الفصل الخاص بهذه الأقمار أي بالتقاط

الموجات الخاصة بهذه الاتصالات إما مع قمر اصطناعي مجاور لقمر الاتصالات أو بالتقاط الاتصالات بواسطة محطات أرضية خاصة مزودة بهوائيات عملاقة لاستقبال الموجات اللاسلكية.

إلا أن جزءاً هاماً من الاتصالات الدولية تتم عبر الاسلاك التي يجري مدها تحت البحار؛ والاسلاك تحت البحار تكون إما معدنية تقليدية أو مصنوعة من الألياف الزجاجية، وطريقة التنصت على الاسلاك المعدنية مماثلة لطريقة التنصت على الاسلاك المعدنية البرية، وتختلف عنها فقط بوجوب استعمال غواصات لتركيب خطوط التنصت تحت سطح البحر.. أما مهمات التنصت إلى الاتصالات التي تتم بواسطة اسلاك مصنوعة من الالياف الزجاجية فهي عملية معقدة بالنظر إلى استحالة تركيب سلك تحويلي عليها...

ومع ذلك فإنه بات من المؤكد أن وكالة «ان أس آي» قد تمكنت من التجسس على الاتصالات في الاسلاك البحرية بالألياف، أما التقنيات المعتمدة حالياً لهذه الغاية فتقضي بإحداث ثقوب صغيرة في الأسلاك لالتقاط الأشعة البصرية التي تعبر فيها، أو بالتقاط الاشارات الالكترونية المنبعثة عن معدات تكبير الأصوات على الشبكة الهاتفية البصرية، على أن التقنيتين معقدتين ويصعب القيام بالأعمال التي تتطلبها من دون لفت انتباه الشركات التي تستثمر شبكة الاسلاك، وهذا الأمر يجعل وجود اتفاقات سرية بين هذه الشركات وبعض

وكالات المخابرات أمراً مرجحاً خصوصاً وأن هذه الوكالات قادرة على ممارسة الضغوطات على شركات الاتصالات والشركات الصانعة للمعدات المعتمدة.

والضغط هذا يتم بالترهيب أو بالترغيب، والترهيب يكون بتهديد المسؤولين فيها بملاحقتهم قضائياً، (مثلاً لقضايا تتعلق بالتهرب من تسديد الضرائب على الدخل...) أو بالضغط على الحكومات لكي لا تمنحها اجازات بفتح الخطوط؛ أما الترغيب، فيكون باستئجار خطوطها وبمساعدة شركات الاتصالات على الفوز بعقود دولية، وكذلك بشراء المعدات من الشركات الصانعة لها..

هذا وتجدر الاشارة إلى أن بعض المصادر أفادت بأن الوكالة البريطانية المتخصصة في التنصت على الاتصالات قد انفقت نحو 100 مليون جنيه استرليني في السنوات الأخيرة من أجل تطوير تقنية اقتصادية تتيح التقاط الموجات على الأسلاك البصرية، وباءت جميع جهودها بهذا الصدد بالفشل الذريع (على ذمة ما تذكره مصادر صحافية بريطانية على الأقل...).

أما بالنسبة إلى وكالة الأمن القومي الأميركية، فتقول بعض المصادر العلمية بأن مهندسي الوكالة ابتكروا نظاماً جديداً يتيح تحويل البيانات في الموضع الذي يتم فيه توجيه الاتصال إلى النقطة المطلوبة، وتقول مصادر أخرى بأن الوكالة لا تحتاج إلى ابتكار

تقنيات خاصة بها، بل انها اكتفت بعقد اتفاقات مع الشركات الأميركية التي تتولى استثمار الاتصالات، وان هذه الاتفاقات تسمح لها بتركيب معدات التنصت في مراكز التحويل بصورة مباشرة، مع العلم بأن هذا السلوك ليس بالأمر الجديد على الوكالة التي سبق لها وأن أبرمت اتفاقات مماثلة في الخمسينات والستينات.

أما في ما يتعلق بالاتصالات الهاتفية الخليوية (أو الخلوية) فإن هذه الاتصالات تتم عن طريق تبادل موجات لاسلكية بين محطات أو خلايا (Cells) مع تحويل الاتصالات بواسطة مركز تبديل عام.

ومن الناحية التقنية، فإن الموجات اللاسلكية الخلويةتعمل بطريقتين: إما بتقنية قياسية (analog)، أي أن بيانات الاتصالات تبث كما هي، ويسهل حينها التقاطها بواسطة معدات لتلقي الموجات. والطريقة الثانية هي التقنية الرقمية (digital)، وهي الأكثر شيوعاً في يومنا الحاضر، وذلك بالنظر إلى دقة وجودة الاتصالات بهذه الطريقة.

ويتم تشفير بيانات الاتصالات بالتقنية المرقمة مع فك التشفير على مستوى محطتي البث والاستقبال، وهذا يعني أن التقاط البيانات على مستوى بثها «على الهواء» لا يفيد الجهة المتنصِتة (بكسر الصاد) بشيء بالنظر إلى صعوبة فك الشيفرة. وتتم عملية التنصت إذ ذاك على مستوى خلايا توصيل الاتصال وعلى مستوى مركز فرز

وتبديل الاتصالات (أي على مستوى «السنترال»)، وأعمال التنصت هذه معقدة من الناحية التقنية، ومرتفعة الثمن من الناحية المالية، ولذلك من المُفضل أن يكون قد أُبرم اتفاق بهذا الصدد بين الشركة التي تؤمن الاتصالات والجهة التي تقوم بأعمال التنصت، على غرار ما سبق وذكرناه بخصوص الاتصالات بالأسلاك الهاتفية البحرية. ولا بد من الاشارة إلى أن تقنية الاتصالات الخليوية تتطلب تحديد المواقع التي تتواجد فيها الأجهزة الهاتفية في طرفي الاتصالات، وذلك لكي يتمكن نظام التبديل الآلي من توجيه الاتصال وتأمينه ويعني هذا أن جهة تراقب الاتصالات الخليوية ويكون لها ولوج مباشر إلى مركز التبديل تستطيع أن تحدد أماكن تواجد المتصلين، وليس فقط لتستمع للاتصالات، مع الاشارة إلى أن السلطات الروسية تمكنت من قتل زعيم جماعة الشيشان جوهر دوادييف في نيسان (ابريل) 1996 بقصف مقره بعد أن تم تحديد موقع هذا المقر عن طريق مراقبة اتصالاته الهاتفية الخليوية عندما كان يجري اتصالاً مع المغرب (بواسطة الاقمار الاصطناعية).

كما نذكر أن الشركة اليابانية للاتصالات ان تي تي (NTT) بدأت تطرح خدمة هاتفية خليوية تتيح تحديد أماكن تواجد حاملي أجهزة الهاتف الخليوي ضمن نطاق لا تتجاوز مسافته 50 متراً.

وتعمل هذه الخدمة عن طريق وضع برامج خاصة داخل أجهزة

الهاتف، وهذه البرامج تعتمد على نظام جي بي اس (GPS) وعلى برامجيات خاصة من شركة سنابستراك (Snaspstrack) الأميركية، حيث أن هذه البرامج تؤمن تحليل الاشارات الكهرومغناطيسية المنبثقة من الجهاز الخلوي لتحديد موقع تواجد الجهاز.

ومن الناحية المبدئية، فإن الهدف من طرح هذه الخدمة هو جعل الشركات قادرة على مراقبة حركات الموظفين لديها خلال ساعات دوام العمل، إلا أن العديد من جمعيات الحفاظ على الحقوق الانسانية أبدت تخوفها من أن يؤدي انتشار هذا النظام إلى التعرض لقدسية الحياة الخاصة وإلى وضع أسس متينة لاقامة نظام بوليسي.. علماً بأن القوانين اليابانية لا تتضمن ما يمنع استعمال هذا البرنامج:

شبكة الانترنت: وأما بالنسبة إلى شبكة الانترنت، يؤكد عميل سابق لوكالة الأمن القومي الأميركية بأن هذه الأخيرة تقوم بمراقبة حركة البيانات في المواقع الرئيسية بالتواطوء مع الشركات الرئيسية التي تقوم بتزويد الخدمات على الشبكة، ويُرجح بأن تكون الوكالة نجحت في التوغل إلى العديد من هذه المواقع وإلى زرع الفيروسات أو برامجيات التنصت والمراقبة فيها وبعض هذه الفيروسات قد يتيح للوكالة مراقبة محتويات أجهزة الكمبيوتر المرتبطة بالمواقع مع فحص محتويات ذاكراتها.

وهناك بعض فئات الاتصالات التي يستحيل التقاطها إذا لم تكن

الجهة التي تريد القيام بأعمال الالتقاط على مقربة من احدى النقاط التي يتم فيها الاتصال،.وخصوصاً في ما يتعلق بالاتصالات اللاسلكية بالموجات القصيرة، ولهذا السبب، انشأت وكالتا أن أس آي وسي أي آي الأميركيتان هيئة مشتركة في ما بينهما تعرف بـ «خدمة الجمع الخاصة» (Special Collèction Service) متخصصة بتركيب أنظمة للتنصت خارج أميركا على مقربة مى مصادر الموجات القصيرة للاتصالات؛ والعاملون في هذه الهيئة يعملون بتغطية ديبلوماسية، ومراكز التنصت كائنة داخل مباني السفارات والقنصليات والمراكز الثقافية الأميركية، ويمكن أن يكون هؤلاء من العاملين في المنظمات التابعة لهيئة الأمم المتحدة، والمثال البارز على هذا الصعيد هو منظمة الأونسكوم التي كانت تضم «مراقبي الاسلحة العراقية»، حيث أقر بعض هؤلاء بأنهم يعملون في الواقع لحساب هيئة سي آي أي وجهاز الموساد اليهودي وكذلك بعض منظمات الاغاثة ذات الطابع الدولي، وقد انكشفت ارتباطات بعض تلك الجماعات مع هيئات المخابرات (يُراجع بهذا الصدد كتاب «ملف اللوبي اليهودي في العالم»).

الفصل الخامس:

تحليل ومعالجة بيانات التجسس والتنصت

بعد أن يتم جمع البيانات بواسطة الأنظمة المختلفة، كيف تتم معالجتها وكيف يتم فرز المهم فيها عن البالي؟

نتناول في ما يلي الوسائل التي يعتقد بأن وكالة الأمن القومي الأميركية تعتمدها في هذا المجال، مع التذكير بأن هذه الوكالة هي الأبرز العاملة في هذا المجال، وبأن معظم وكالات المخابرات العالمية تعتمد على وسائل مشابهة.

فيما يتعلق بالاتصالات الهاتفية المطلوبة معالجتها، فان الجهات التي تتولى التقاطها تقوم بترقيمها من مركز عملها حيث يتم استقبال بيانات الاتصال، وبعد ذلك تُرسل شيفرة الاتصال إلى مقر وكالة ان أس آي بواسطة أسلاك خاصة محصنة ويفترض انه يستحيل خرقها. أو بالاقمار الاصطناعية. وتتم عملية الفرز عن طريق فحص مصادر الاتصالات، حيث تتولى

الوكالة مراقبة بعض الهيئات بصورة محكمة وشاملة، وخصوصاً السفارات والقصور الرئاسية والوزارات في البلدان المستهدَفة (بفتح الدال).

ولدى الوكالة برامج كمبيوترية قادرة على تصنيف الاتصالات الصوتية حسب الصوت مع التعرف أوتوماتيكياً على أصوات أشخاص تُراد مراقبتهم.

وهناك برامج أخرى تتيح تحديد أسماء أو كلمات تهم الوكالة بصورة أوتوماتيكية، وهو ما يؤدي إلى معالجة الاتصالات التي يتم فيها ذكر هذه الكلمات. كما لدى الوكالة برامج لترجمة أكثر من 100 لغة إلى الانكليزية بصورة أوتوماتيكية (اشارة هنا إلى عدم دقة برامج الترجمة الآلية بصورة عامة، مع ضرورة ارفاقها بعملية تدقيق يتولاها ترجمان متخصص في حال كانت المكالمة ذات أهمية حيوية).

التقنيات التي تستعملها وكالة أن أس آي: تؤكد المصادر العليمة بأن وكالة أن أس آي تقوم برعاية تطوير أجهزة السوبر كمبيوتر المتفوقة عن طريق تمويلها من ميزانيتها الخاصة (وكذلك الأمر مع الأقمار الاصطناعية وأجهزة التنصت المختلفة....).

وتستعمل الوكالة بصورة رئيسية أجهزة سوبركمبيوتر من شركة كراي (Cray)، ويتم صنع شرائح هذه الأجهزة في مصنع

سري خاص بالوكالة.

تسعى الولايات المتحدة للحفاظ على تفوقها التقني بتطوير تقنيات ومعدات للالتقاط شديدة التعقيد والحساسية، مع تمويل وكالة أن أس آي عملية تطوير نظام كمبيوتري يعمل بالأشعة الكنتية (quantum rays) وتصل قوة ادائه إلى ما يوازي ملايين اضعاف قوة معالجة أجهزة السوبر كمبيوتر من كراي...

هل يعني كل ذلك أن أميركا باتت قادرة على معرفة كل شاردة وواردة في العالم بأجمعه؟

الجواب هو لا والسبب بكل بساطة هو أن تلك الكمية الهائلة من البيانات المخابراتية التي تأتي إلى الوكالات الأميركية تعرقل فعالية نشاطات الفرز والمعالجة، حيث يستحيل معالجتها بصورة مجدية مع العلم بأنه يتم في كل عام إتلاف الف طن من المستندات في وكالة أن أس آي ،على أقل تقدير، بواسطة محلول كيميائي خاص. والواقع أن هيئات المخابرات الأميركية قد عرفت عدة حالات فشل في المدة الأخيرة مثل عدم التمكن من توقع اجراء الهند لتجاربها النووية أو عدم الحؤول دون تفجير السفارات الأميركية في كل من كينيا وتانزانيا سنة 1998.

من ناحية أخرى، يتزايد اهتمام الشركات الخاصة بتقنيات التجسس واخفاء المعلومات، وأدى ذلك إلى تطوير أنظمة معقدة

للتشفير ولتشويش البيانات وهي مطروحة في المتاجر بأسعار معقولة وتسعى وكالة أن أس آي إلى الحد ما أمكن من تفشي هذه الأنظمة، وهي نجحت في فرض قيود صارمة في الولايات المتحدة على تقنيات التشفير، مما يسمح لها بالتعرف على المعاني الحقيقية للبيانات المشفرة، كما أن عدة دول رضخت للضغوطات الاميركية ووافقت على تقييد ومراقبة تصدير برامج تشفير البيانات التي يزيد طولها على 64 بت (bits)، الا أن العديد من البلدان الاخرى لم تخضع لهذه القيود...

كذلك يتزايد عدد الشركات الخاصة والدول التي تطرح بيع الصور التي تلتقطها الاقمار الاصطناعية التصويرية على أي كان يدفع ثمنها، وهو الأمر الذي يكسر احتكار أميركا للحصول على صور متقنة.

خلاصة القول أن الولايات المتحدة هي من دون شك القوة المخابراتية الأكبر في العالم بالوقت الحاضر (أي في سنة 1999)، إلا أن قدرتها ليست مطلقة حيث بدأت أكثر من دولة وشركة خاصة تطور تقنيات يمكن من خلالها أن يُصار إلى التصدي للتفوق الاميركي، وهو ما نبينه في الفصول المقبلة.

ملحق

اعتماد المخابرات الأميركية على مناجم البيانات

بدأت وكالات المخابرات الأميركية تتخذ الخطوات العملية لتطبيق نظرية «المصادر المفتوحة للمعلومات» وخصوصاً لجهة أخذ المعلومات من شبكة وب (web)مع فرز المعلومات بغية عدم الغرق في محيط من التفاصيل غير النافعة.

وتقنية «المناجم البيانية» (data mining) باتت احدى الأدوات الأساسية التي تعتمد عليها وكالة سي آي أي لتحليل المعلومات التي تتلقاها.

و«مناجم البيانات» كناية عن استعمال البرامج الكمبيوترية لاستكشاف كمية كبيرة من المعلومات المخزنة في ذاكرة الكمبيوتر وتصنيفها واختيار المناسب منها مع إمكانية دراسة النتائج المترتبة على تفاعل جميع هذه العوامل المتفاوتة. ويلعب الكمبيوتر دوراً رئيسياً هنا بالنظر إلى أن حجم المعلومات المتوافرة اليوم حول مختلف المواضيع يبلغ قدراً لا يمكن معه استغلالها وتحليلها بصورة مباشرة من قبل الخبراء. ويدل ذلك على أن هذه «الثروة» من المعلومات باتت تشكل عائقاً أمام اتمام العمل المجدي، وليس العكس، وهو ما يستتبع ضرورة الاستعانة بطريقة «مناجم البيانات» الكمبيوترية.

وباشرت وكالة سي آي اي تستعمل بهذه الطريقة في معالجة مواضيع متعددة، ومن أبرزها:

- وضع خطط المعارك العسكرية.

- دراسة حركة تجارة السلاح في العالم.
- انتشار أسلحة الدمار الشامل.
- الاتجاهات السياسية في العالم.
- مراقبة كيفية استعمال الموظفين في الدوائر والشركات لأجهزة الكمبيوتر الخاصة بالدوائر، للكشف عن الجواسيس.

تجدر الاشارة إلى أن الشركات الكبرى في الدول الصناعية الغربية هي التي ابتكرت وطبقت هذه التقنية، إلا أن المعضلة الكبرى بالنسبة إلى وكالة المخابرات الأميركية تتمثل بوجوب مراعاة شروط المحافظة على مستويات الأمن السرية عند معالجة المعلومات ونشرها بغية استغلالها.

وذكر مصدر مسؤول في الوكالة بأن «التحدي الأول بالنسبة إلى الوكالة هو ضمان حصول المحللين على جميع المعلومات التي يحتاجونها دون الغرق في سيل من المعلومات الفائضة، ولقد بدأنا نعتمد على نموذج «وب» (Web) كطريقة لجمع وحفظ واستخراج وثائق المعلومات».

ويمكن تلخيص الفلسفة الجديدة للوكالة في مجال جمع المعلومات بوجوب وضع جميع البيانات داخل مواقعها على الانترنت، مع إمكانية الولوج إليها بواسطة الشبكة الداخلية الخاصة بالوكالة من ضمن الانترنت وتعرف بشبكة «سي آي ايه لينك» (CIA Link). إلا أن هذه الطريقة لا تحل وحدها مشكلة تضخم حجم المعلومات الواردة، حيث تبين أن هذا الحجم يتضاعف مرة كل خمس سنوات بسبب تزايد عدد مصادر المعلومات الناجم عن الانتشار الواسع الذي عرفته شبكة الانترنت، كما يصعب على الوكالة أن تقوم بعملية فرز وتصنيف

المعلومات بين سرية وعلينة لدى اعتماد هذا الاسلوب.

وأقامت الوكالة في سنة 1996 مكتباً مخصصاً لتطوير ادوات معلوماتية متقدمة لتحليل البيانات، وتقوم مديريتا المعلومات والعلوم والتكنولوجيا في الوكالة بادارته.

وأمام هذا المكتب تحقيق هدفين رئيسيين يتمثل الأول بتحديد الطريقة التي تؤمن حصول المعلومات بطريقة ميسرة من قبل جميع من يحتاج إليها، والثاني بجعل الأدوات البرامجية الكمبيوترية تقوم بأعمال الفرز بصورة أوتوماتيكية.

هذا، وترغب الوكالة في أن تكون كل البرامج المطلوبة معتمدة على تكنولوجيا تستعمل في القطاع الخاص وأن تكون سهلة الاستعمال. ويبقى الهدف الأول للوكالة هو الحصول على معلومات تكون مفيدة حقاً، وليس فقط على تكديس البيانات مع العجز عن استغلالها بالطريقة المناسبة.

الفصل السادس:

وكالات المخابرات تسعى للسيطرة على أدمغة أعدائها

هناك حلم قديم يراود مخيلة مؤلفي روايات وأفلام العلم الخرافي، وهو بأن تتمكن جهة ما من السيطرة على الأدمغة لقراءة الأفكار وكشف الأسرار، فضلاً عن امكانية اجراء الاتصالات عن طريق توارد الأفكار، أو املاء الآراء والقناعات على أذهان الخصوم.

والواقع أن هذه التصورات خرجت الآن عن مجرد نطاق الوهم ودخلت مجال التجارب والاختبارات العلمية، حيث أن عدة وكالات مخابراتية تدرس إمكانية استعمال الدماغ البشري كجهاز معلوماتي، ولم تعد تحصر جهودها بتطوير التكنولوجيا، وتصميم أجهزة جديدة، وإنما تتعاون بصورة مكثفة مع مراكز الابحاث البيولوجية للتعرف على أسرار الدماغ وعلى كيفية استغلاله بما يخدم تحقيق أهداف العمليات المخابراتية.

وهناك غطاء كثيف من السرية يكتنف هذه الأبحاث، وهو ما تسبب في اطلاق شائعات عديدة حول حقيقة الأبحاث الدائرة والتجارب التجارية بهذا الشأن، إلا أنه أمكن الحصول على عدد ضئيل من المعلومات شبه الأكيدة بهذا الشأن نسعى هنا إلى استعراضها بكل تحفظ، مع محاولة استشراف الآفاق المستقبلية لهذه الأبحاث.

المعطيات العلمية المعروفة حول الدماغ: هناك أكثر من طريقة للتحكم بالدماغ، أو بالأحرى للتأثير عليه: هناك طريقة «التنويم المغناطيسي» وإملاء الأفكار، وطريقة التقاط الموجات الكهرومغناطيسية التي يبثها الدماغ، وطريقة تلقين الشخص المطلوب السيطرة على دماغه بالمخدرات، وخصوصاً المخدرات الكيميائية الاصطناعية.

في ما يتعلق بطريقة التنويم المغناطيسي وإملاء الأفكار، فهناك أبحاث علمية تجرى بهذا الصدد في مراكز الأبحاث الطبية منذ أواخر القرن التاسع عشر، مع السعي لاستغلال هذه الأبحاث في الطب النفساني بصورة رئيسية، وأبدت وكالات المخابرات اهتماماً بالغاً بهذه الأبحاث والتجارب منذ بداياتها، وقامت بإجراء التجارب وبدعمها وتمويلها، وكانت الوكالة المخابراتية الروسية القيصرية «الأوكرانا» من بين أكثر من اهتم بالأمر، وذلك منذ أوائل القرن العشرين، وخلفتها في ذلك أجهزة مخابرات الاتحاد السوفياتي، وتؤكد عدة مصادر بأن الروس مايزالون نشيطون بهذا الشأن حتى يومنا الحاضر. كذلك فمن الأمور الثابتة أن الوكالات المخابراتية

الأميركية والأوروبية أولت هذا الشأن أهمية كبرى.

بيد أن الأمر الثابت هو أن هذه الأبحاث لم تعطِ نتائج عملية كبيرة، ولذلك فإن التركيز هو على التقاط الموجات الكهرومغناطيسية المنبعثة من الدماغ.

والمعروف أن الموجات الكهرومغناطيسية قادرة على اجتياز مدار الكرة الأرضية عدة مرات في غضون ثانية واحدة عندما يتم بثها على ذبذبة تساوي صفر هيرتز، ولا تحتوي هذه الموجات على طاقة كهربائية وهي حيادية من ناحية التيار الكهربائي، كما أنها قادرة على الدخول في جميع أنواع المواد، مثل المياه (لذلك تستعمل هذه الموجات لاجراء الاتصالات السرية مع الغواصات النووية) وكذلك الغطاء الرأسي للانسان. ولقد اكتشف العلماء بأن الدماغ يعمل عن طريق بث واستقبال موجات كهرومغناطيسية، وبالتالي فإن اكتشاف طول هذه الموجات يسمح بالتأثير على تصرف شخص يتم توجيه الموجات إليه.

والواقع أن الطب الدماغي يستعمل آلات تبث مثل هذه الموجات لمعالجة أمراض مثل الصرع، كما أنه تم صنع أجهزة لتحليل هذه الموجات ومعالجتها خلال عمليات استجواب الاشخاص المشبوهين في البلدان الغربية ومعرفة ما إذا كانوا يجيبون بالكلام الصحيح أو الكاذب، وتُعتمد هذه الأجهزة بصورة مكثفة في بعض وكالات المخابرات في البلدان الصناعية، وخصوصاً في الولايات المتحدة وذلك على الرغم من أن العديد من العلماء يشككون في صحة الاستنتاجات التي يمكن التوصل إليها لهذه الطريقة.

ولقد أُجريت بعض الاختبارات التي أتاحت بث موجات كهرومغناطيسية وتوجيهها إلى دماغ شخص موضوع الاختبار، وأمكن تحويل بعض الكلمات المفهومة إلى هذا الدماغ على ذمة ما تؤكده بعض المصادر غير المؤكدة.

غير أن الطريقة الأكثر «اعتمادية» لنقل الأفكار مباشرة إلى الأدمغة تكمن في زرع معدات الكترونية في رؤوس الأشخاص المطلوب التأثير عليهم وبث توجيهات إليها تلتقطها تلك المعدات بصورة أكيدة، وتعيد بثها إلى خلايا الدماغ ليتم تسجيلها وتنفيذها، وبكلام آخر يتم املاء الأفكار بواسطة الجهاز المزروع في الرأس.

ويؤكد بعض الأشخاص بأنه قد تم زرع مثل هذه الأجهزة في رؤوسهم من دون علمهم، وأنهم يعانون من آلام مبرحة لهذا السبب، وهناك مواقع مخصصة لهذا الموضوع على شبكة الانترنت، حيث تعرض صور بأشعة الاكس للأجهزة المزروعة، ولو أنه يصعب التأكد من صحة هذه الادعاءات، والأمر الثابت الوحيد هو أن المستوى الحالي للجراحة والطب (في سنة 1999) يسمح بزرع أجهزة صغرية في الدماغ، أما في ما يتعلق بالنتائج العملية لهذه العمليات، فإنها تبدو محدودة للوهلة الأولى، بدليل أن من يدعون أنهم تعرضوا لعمليات الزرع يحتجون عليها بدلاً من ينصاعوا بصمت لادارة من أراد أن يتحكم بأفكارهم.. إشارة هنا إلى أن جمعية تشكلت في أسوج من أجل العمل على وضع حد لهذا النوع من التجارب المخالف لشرعة حقوق الانسان، وأن هذه الجمعية أكدت بأن عمليات من هذا النوع

تمت في كل من الولايات المتحدة والمانيا وأسوج والدانمارك وبريطانيا، مع تحديد هذه الحالات... ولقد جرى تكذيب المعلومات التي كشفتها الجمعية من قبل الوكالات المخابراتية موضوع الاتهام، أوأنه تم تجاهلها مع عدم التعليق عليها...

هذا في ما يتعلق بالسيطرة على الدماغ عن طريق التكنولوجيات الالكترونية. أما في ما يتعلق بالسيطرة على الدماغ بواسطة الأدوية والمخدرات، فمن شبه الثابت أن دوائر المخابرات الأميركية والبريطانية (وكذلك الوكالات الروسية والفرنسية ووكالات بلدان متقدمة أخرى على الأرجح) قد أجرت تجارب مكثفة (وما تزال) حول مفاعيل المخدرات الكيميائية المركبة مثل مخدر ال أس دي(LSD) وغيرها، وقد أدت بعض هذه التجارب إلى حصول حالات انتحار أو وفيات فجائية. وتتركز الأبحاث والتجارب الأميركية بهذا الصدد على استعمال أدوية تستعمل عند اخضاع المتهمين للاستجوابات وتتسبب بأن يدلي الشخص المستجوَب بكل ما لديه بدقة وبكل صدق من ناحية، وبأن ينسى هذا الشخص ما حصل معه أثناء الاستجواب بصورة كاملة في ما بعد. ويصعب معرفة ما إذا كانت التجارب أعطت نتائج ذات مغزى، إلا أن الأمر الثابت هو أنه جرى التحدث عن بعض الحالات اللافتة، ومن ذلك أن طيارين أوروبيين كانوا يشتركون في مناورات مشتركة في الولايات المتحدة اضطروا إلى الهبوط في مطار أميركي يتم فيه اختبار الطائرات السرية «الخفية» (Furtive)، وذلك بسبب أعطال طرأت على طائراتهم، مع حصول عملية الهبوط على الرغم من أن المطار رفض منح

الاذن بذلك رفضاً تاماً.

وعند عودة هؤلاء الطيارين تبين أنهم كانوا في حالة ضياع استمرت لبعض الوقت، ولم يعودوا يتذكرون شيئاً مما حصل لهم بعد عملية الهبوط، وخصوصاً في ما يتعلق بالطائرات السرية في المطار، وقد يكونوا خضعوا لهذا النوع من المعالجات بالأدوية والمخدرات.

كما تمت عمليات لدراسة مدى إمكانية استعمال الأدوية والمخدرات للتأثير على تصرف الشخص الذي يكون قد تناولها، وتقول بعض المصادر بأن وكالة سي آي أي تستعمل بعض الشيع «الدينية» (Sects) في أميركا والعالم كغطاء لاجراء التجارب.

خلاصة القول أن التجارب على الدماغ وعلى كيفية التحكم به عن بعد جارية بصورة مكثفة وأن الدوائر المخابراتية أكثر من يهتم بهذه الأبحاث والتجارب: ولم تعط الأبحاث نتائج حاسمة حتى الآن على ما يبدو، إلا أن الأبحاث تتم على خطوات حثيثة وقد لا يكون بعيداً اليوم الذي تتمكن فيه دولة متقدمة ما من زرع دماغ رئيس دولة أخرى بجهاز الكتروني تتمكن بواسطته من السيطرة عليه، وذلك بمناسبة خضوعه للعلاج الطبي في تلك الدولة المتقدمة.

والرد المناسب على هذه المخاطر يكون بإجراء كل دولة تريد الحفاظ على سيادتها وحرية قراراتها أبحاثاً خاصة بها في هذه المجالات من جهة، بالحؤول دون تلقي المسؤولين فيها للعلاج الطبي في بلدان أخرى من جهة أخرى.

الفصل السابع:

أنظمة الرقابة الخاصة بالمدنيين

من الواضح أن نشاطات التجسس لم تعد تنحصر على المجالات الاستراتيجية العسكرية والسياسية، أو تلك الخاصة بالشركات الكبيرة، بل انها باتت تشمل جميع جوانب الحياة اليومية للافراد، من مراقبة لحركة السير إلى تسجيل المكالمات الهاتفية على صعيد افرادي إلى مراقبة العمال في المصانع وغير ذلك... ونتطرق هنا إلى الامكانات العملية الخاصة بتلك الأنظمة «الافرادية» وإلى التقنيات المعتمدة.

الامكانات التي توفرها التقنيات الحديثة:

هناك تقنيات تتيح القيام بأعمال مراقبة محكمة في جميع جوانب الحياة اليومية، ومن ذلك أمثلة بسيطة من قبيل مراقبة حركة الزبائن في المتاجر الكبرى بواسطة كاميرات خاصة لكشف السارقين، وذلك عن طريق مراقبة تصرفات الزبائن من ناحية، أو عن طريق مقارنة ملامح وجوه هؤلاء الزبائن مع ملامح سارقين معروفين تكون مخزنة في قاعدة بيانات كمبيوترية، مع اتمام

عملية المراقبة بصورة أوتوماتيكية، وبسرعة لمح البصر؛من ناحية أخرى ؛ كما يمكن مراقبة المعالجات التي تتم على أجهزة الكمبيوتر الشخصية في منزل خاص عن طريق التقاط الموجات الكهرومغناطيسية المنبعثة عن الكمبيوتر خلال عمله، مع إمكانية اخفاء المعدات المستعملة لاجراء عملية الالتقاط في شاحنة فان صغيرةمتوقفة على مقربة من مكان الكمبيوتر...

كما أن هناك شرائح الكترونية صغيرة غير قابلة للكشف يمكن زرعها في الأجهزة الهاتفية، وتتيح هذه الشرائح تسجيل جميع الأصوات في الغرفة التي يوضع فيها جهاز الهاتف، وبثها باتجاه مركز للاستقبال، وتوصيل الموجات اللاسلكية.

والواقع أن انتشار نشاطات الرقابة بلغ حداً حوّل التساؤل الشائع عند الناس في ما إذا كانوا عرضة أم لا إلى أعمال الرقابة إلى تساؤل آخر هو: هل أن ثمة من يكترث فعلاً بالبيانات الرقابية التي يتم جمعها حولهم؛ بمعنى آخر فإن جميع الناس باتوا معرضين لأعمال الرقابة، وإنما بدرجات متفاوتة...

فلقد أتاحت الأنظمة الالكترونية والمعلوماتية ممارسة أعمال الرقابة بمجرد استعمال هذه الأنظمة، ومن الأمثلة على ذلك استعمال البطاقات الائتمانية لسحب النقود وتسديد الحسابات أو الاطلاع على مواقع شبكة وب (أي شبكة الانترنت) ، واستعمال

الهاتف الخليوي حيث تؤدي كل واحدة من هذه الأعمال إلى الاتصال بقاعدة بيانات مركزية يتم فيهاتحديد مصدر الاتصال ونوعية الحركة، مع امكانية تشديد مدى المراقبة..

والمشكلة بالنسبة لمن يريد الحصول على المعلومات المحصلة عن طريق أعمال الرقابة ليست في كيفية جمع المعلومات، وانما في كيفية معالجتها لكي تعطي نتيجة مجدية. وتقدم في ما يلي نبذه حول بعض أبرز التقنيات المعتمدة في يومنا الحاضر مع أهم تطبيقاتها:

أبرز تقنيات الرقابة في القطاع المدني:

- أنظمة الرقابة على الأفراد: من الأمثلة على تلك الأنظمة نظام فاسيلت دي بي (FaceIt DB) للتعرف على ملامح الوجوه وتطرحه الشركة الأميركية فيزيونيكس (Visionics) (سنة 1998) ، هذا البرنامج يتيح تفحص وجوه المارة ضمن مجموعة من الناس ومقارنتها مع ملامح مخزنة في قاعدة للبيانات، وذلك عن طريق استعمال الطريقة الاحصائية لدراسة تفاصيل كل موضع من مواضع الوجه، وبعد ذلك يتم جمع الخصائص الاحصائية لهذا الوجه لمعرفة ما إذا كانت هذه الخصائص مطابقة لخصائص ملامح شخص آخر تكون مخزنة. والبرنامج قادر على التعرف على الوجوه من زوايا تصل إلى 35 درجة، مع الأخذ بعين الاعتبار

عوامل الاضاءة ولون الشعر والسن وانعكاس المشاعر وغير ذلك. ويمكن استعمال النظام للتدقيق في المواقع والاوقات التي يتنقل فيها الشخص الذي تجري مراقبته. ومن الأمثلة الأخرى نظام بريطاني يستعمل طريقة الذكاء الاصطناعي لتعقب الأشخاص الذين يتحركون في مواقف السيارات بصورة أوتوماتيكية مع التعرف على من يتصرف بطريقة مشبوهة قبل ارتكاب أعمال مخالفة للقانون، وتقضي هذه الطريقة بمراقبة مواقف السيارات مدة طويلة لدراسة طريقة التصرف، وبعد ذلك تخزين أوجه التصرف المشبوهة في ذاكرة الكمبيوتر .وبعد اتمام عملية الدرس والرقابة، يتم التعرف إلى التصرفات المشبوهة بصورة دقيقة، واذا تبين في ما بعد بأن شخصاً ما يتصرف على هذه الشاكلة يتم انذار حارس الموقف، وهو يتولى التحقيق مع الشخص المشتبه به، و أجريت تجارب تعتمد على هذا النوع من البرامج في عدد من الدول من أجل السعي إلى خفض عدد الجرائم، إلا أن النتائج لم تكن مرضية في كل الحالات، حيث لاحظت شرطة مدينة ميامي الأميركية على سبيل المثال بأن هذه الطريقة أدت بالفعل إلى تراجع النشاط الاجرامي في المناطق التي تجري مراقبتها، إلا أن ذلك أدى إلى تنامي الاجرام في المناطق غير المراقبة فتكون المشكلة قد انتقلت من منطقة إلى أخرى وحسب...

ـ وهناك تقنية مشابهة لمراقبة ومقارنة الأصوات التي تثير الريبة

من قبيل صوت طلق ناري على سبيل المثال؛ ويتم وضع ميكروفونات في الأماكن العامة مرتبطة بأنظمة كمبيوترية تابعة للشرطة، وهذه الأنظمة الكمبيوترية تكون مزودة بقواعد بيانات تخزن فيها الأصوات المشبوهة، فإذا صدرت إحدى هذه الأصوات يتم تحديد الموقع الذي انطلقت فيه ومن ثم ترسل دوريات إلى هذا المكان.

ولهذا النظام تطبيقات عسكرية، حيث يتم استعماله لتعقب القناصين، كما يمكن تطويره للرد باطلاق النار اوتوماتيكياً.

كما أن هناك برامج للتعرف على الصوت تتيح التعرف أوتوماتيكياً على نداءات الاستغاثة مع تحديد مواضعها.

- زرع الشرائح الالكترونية في أجساد الاشخاص: من المعروف أنه يتم زرع شرائح الكترونية في جلد بعض الحيوانات الاليفة، ولا سيما منها الكلاب من أجل معرفة أماكن تواجدها وتفادي سرقتها؛ هناك اقتراح بأن يتم أيضاً زرع مثل هذه الشرائح الالكترونية لدى الأفراد، بحيث تبث اشارة خاصة بصاحبها، ويمكن استعمال هذه الطريقة لكي تخزن المعطيات الالكترونية الخاصة بصاحب الشريحة، من قبيل أرقام الهاتف والبطاقة الائتمانية وضبط مقاعد السيارة إلخ.... بحيث يتم تشغيل هذه التسهيلات بصورة أوتوماتيكية بمجرد اتصال

الشـريحـة لاسـلكياً بـالجـهـاز الـخـاص، (مـثـلاً لطلب عنوان للبـريد الالكتروني بصـورة أوتوماتيكية مع أي جـهاز كمبيوتر مرتبط بالانتـرنت) لكن بـالمقابل فـإن هذه الشـريحـة يمكن أن تـشكل أداة مثالية للتـجسس على صـاحب الشـريحـة... ذلك أن رقم الشـريحة يمكن أن يعطي وكلاء البطاقات الائتمانية معلومات حول «سـجله» في التـعـاطي مع هذه البطاقـات، أو يمكن التـعـرف إلى جـهـة تنقلاته...

إشـارة هنا إلى أن ادارة السـجـون الأمـيـركـيـة بدأت تعـمـد إلى ربط بعض المحكومين لديها «بسـلاسـل الكتـرونية» هي كناية عن اسوارة الكترونية تتيح تعقب جميع تحركات حامليها، وهو الأمر الذي يسمح باخراجهم من السـجون المزدحمة من دون أن يعني ذلك اطلاق سـراحهم... كما نذكر أن العائلات الاميركية آخذة في تزويد غـرف الأطفـال بكامـيـرات صـغـيـرة يمكن الاتصـال بـهـا بموجـات لاسـلكيـة، مع امكانيـة اخـفـاء الكامـيـرات في ألعـاب أو ساعات جدار على سبيل المثال، وذلك من أجل مراقبة الأولاد عند غياب أوليائهم... ومن الطبيعي أنه يمكن استـعـمـال هذه المعدات للقيام بأعمال أقل براءة من السـهر على الاطفال الصـغار...

أنظمـة التنصت والتـجـسس على الهـاتف: هذه الأنظمـة باتت منتشـرة بصـورة كبيرة في العديد من بلدان العـالم وتتراوح بين

الشرائح التسجيلية والتوصيلية التي يتم زرعها داخل أجهزة الهاتف لتنقل الاتصالات، أو «الشريحة اللامتناهية» (Infinity Bug) وهذه الأخيرة كناية عن ربط جهاز الهاتف المطلوب مراقبته بخط هاتفي إضافي يسمح للقرصان بطلب رقم الخط الاضافي، ليتحول جهاز الهاتف اذ ذاك إلى اداة للتنصت على كل ما يدور في المكان الذي يتواجد فيه الهاتف. غني عن البيان بأنه يصعب تركيب مثل هذا الجهاز في المنازل الخاصة إلا أنه يمكن بسهولة وضعها في غرف الفنادق وقاعات المحاضرات.

من ناحية أخرى، فإن تقنية الاتصالات الهاتفية الخلوية تسمح لمراكز تبديل الاتصالات بتحديد مراكز التحويل التي تم من خلالها توصيل الاتصال الهاتفي، وهذا يعني انه يمكن بكل سهولة تحديد موقع حامل الهاتف، أي أن جهاز الهاتف الخليوي يمكن أن يشكل اداة فعالة للتعقب من قبل الشركات التي تستثمر الشبكات مع العلم أن معظم هذه الشركات تتعاون وتنسق مع وكالات المخابرات كما سبق وأشرنا إلى الأمر.

وأخيراً وليس آخراً، فإن انتشار الكمبيوتر والشبكات الكمبيوترية في المنازل والمكاتب أدى إلى تسهيل أعمال المراقبة حيث من السهل التعرف إلى بيانات البريد الالكتروني، كما يمكن ربط الأجهزة الكمبيوترية بكاميرات للرقابة يمكن تشغيلها عن بعد بواسطة جهاز كمبيوتر آخر...

كل هذا يعني أنه بات بإمكان كل الناس تقريباً القيام بنوع من أعمال التجسس على كل الناس وفي هذا ما يشكل كابوساً مزعجاً عند معظم الناس... بيد أن هذا الانتشار المكثف لأنظمة الرقابة يمكن بدوره أن يؤدي إلى حصول نوع من التوازن بين من يرغب في التعدي على خصوصية غيره والتجسس عليهم، ومن يرفض التعرض لأعمال التنصت والتعقب، والأمر الأكيد هو أن تفشي أنظمة الرقابة على مختلف الأصعدة سوف يكون عاملاً أساسياً لتبديل معالم المجتمع. والسؤال هو: هل أن هذا التبديل سيكون نحو الأفضل أم العكس؟...

ملحق

استعمال الكمبيوتر للتجسس على الموظفين

تعتبر البرامج المعلوماتية المخصصة للتجسس على نشاط مستعملي الكمبيوتر من موظفي الشركات والمؤسسات من أكثر البرامج الأمنية رواجاً في الوقت الحاضر، حيث تطرح عدة تطبيقات معقدة تسمح لأرباب العمل بمراقبة كيفية استعمال الأجهزة الكمبيوترية في مكاتبهم بصورة دقيقة.

ويعود هذا الرواج إلى أنه لوحظ خلال السنوات الأخيرة، أن الموظفين في الشركات يستغلون أجهزة الكمبيوتر الموضوعة تحت تصرفهم من أجل تصفح مواقع ترفيهية على شبكة الانترنت، أو لتبادل رسائل خاصة بواسطة تسهيلات البريد الالكتروني، أو تشغيل برامج للألعاب الفيديوية...

بكلام آخر فإن الكمبيوتر قد تحول هكذا إلى وسيلة لاضاعة الوقت بدل أن يكون أداة فعالة لتعزيز الانتاجية وتحسين نوعية العمل. وتقدر بعض المصادر العلمية الخسائر التي تتكبدها الشركات الأميركية من جراء سوء استعمال الكمبيوتر بمئات البلايين من الدولارات. علماً بأن سوء الاستعمال هذا يمكن أن يكون كناية عن إضاعة للوقت، كما أنه يمكن أن يكون أشد خطورة مثل اقتراف أعمال قرصنة أو تخريب للبرامج المخزنة داخل ذاكرة الكمبيوتر.

ولقد دخلت برامج المراقبة نمط الحياة الاعتيادية للشركات إلى درجة جعلت بعض المدراء يطلعون على البريد الالكتروني الخاص بموظفيهم أو يستمعون إلى محادثاتهم الهاتفية بصورة روتينية، كما

أن بعض الشركات قامت بتركيب آلات تصوير فيديوية في المكاتب لتسجيل كل حركة يقوم بها الموظف.

وقد يقول قائل بأن جميع هذه الممارسات مخالفة لقواعد الحفاظ على سرية الحياة الشخصية، ولشرعة حقوق الانسان، إلا أن هذه الاعتبارات هي في غير محلها بالنسبة إلى الشركات على اعتبار أن مركز العمل مخصص للعمل ولا يجوز ممارسة نشاطات الحياة الخاصة فيه. ويعترف الاختصاصيون في القانون الخاص وفي الدفاع عن حقوق الانسان بصوابية هذه الاعتبارات، ويقرون أن استعمال برامج المراقبة شرعي تماماً ولا يحق لأحد الاعتراض على ذلك..

على أنه لاستعمال برامج المراقبة مفاعيل أخرى تتمثل بأن العمال والموظفين الخاضعين للرقابة سوف يتبرمون من هذا الواقع، وينعكس هذا التبرّم على أعمالهم بحيث يفقدون الحماس وروح المبادرة ويكتفون بأداء أعمالهم بالحد الأدنى المطلوب منهم فقط...

ومن هنا فإن المسألة المطروحة على مسؤولي الشركات هي استعمال برامج الرقابة بطريقة توازن بين ضرورات إنجاز الأعمال ومحاربة الكسل وإضاعة الوقت، وبين وجوب الحفاظ على معنويات الموظفين لكي لا تنعكس سلباً على أدائهم..

الفصل الثامن:

بعض تقنيات معدات التجسس التي يستعملها الأفراد والشركات الخاصة

نتقدم في ما يلي نبذة حول بعض أحدث التقنيات التي تستعمل في أعمال التجسس التي يقوم بها الأفراد أو شركات القطاع الخاص:

الأجهزة اللاقطة للموجات المليمترية:

الموجات الميليمترية (Millimetre- Waves): هي تلك الموجات الكهربائية التي يتراوح عرض نطاق طيفها الكهرومغنطيسي بين ذلك الخاص بالموجات ما دون الحمراء (Infrared Waves) والخاص بالميكروموجات (Micro Waves). وهذه الموجات موجودة في أي شيء يحتوي على الماء، وخاصة الأجسام الحية. والجسم البشري يعتبر من المصادر «النموذجية» لهذه الموجات، ويمكن تشبيهه بالمنارة اللاسلكية (Beacon) المشعة لها.

وتتميز الموجات الميليمترية بقدرتها على اجتياز جميع المواد غير

الموصلة للتيار الكهربائي مثل معظم أنواع أنسجة الملابس ومعظم أنواع مواد البناء. في حين أن المعادن لا تبث إلا قدراً محدوداً من تلك الموجات. أما المواد العازلة (Dielectric) مثل اللدائن (Plastics) والسراميك والمواد المتفجرة فإن بثها للموجات الميليمترية يأتي في الوسط بين المواد غير الموصلة والمعادن. وتتبدل كمية الموجات الميليمترية حسب درجة حرارة المواد التي تبثها. ويمكن تركيز الموجات الميليمترية لتشكل صورة مرئية، تماماً كما هو الحال مع الإضاءة العادية ومع الموجات ما دون الحمراء. ويتم ذلك بواسطة عدسات بلاستيكية. وبدأت تطرح آلات تصوير تعمل بالموجات الميليمترية.

آلات التصوير العاملة بالموجات الميليمترية: من المعروف أنه يتم تحويل الاضاءة إلى إشارة كهربائية في آلات التصوير الفيديوية التقليدية بواسطة مستشعرات على شكل أجهزة مشحونة الكترونياً (Charge Coupled Devices) موضوعة على المسطح البؤري (Focal Plane) لآلة التصوير، حيث تولد إشارة الكترونية تتحول إلى صورة مرئية... وكلما زاد عدد المستشعرات كلما كانت نسبة وضوح آلة التصوير أكثر دقة.

بيد أنه لا يمكن استعمال الأجهزة المشحونة الكترونياً لالتقاط الموجات الميليمترية، وإنما هوائيات لاسلكية لالتقاط انبعاث الموجات

مع وجوب تضخيم التيارات الكهربائية الناتجة عن هذه الموجات لتتحول إلى إشارة الكترونية واضحة، وهذا ما يتطلب استعمال معدات ضخمة الحجم. ولقد توصلت احدى الشركات البريطانية إلى طريقة تصنع هوائيات خاصة بقياس 2 أو 3 ملم. ثم جمع 256 من هذه الهوائيات لتشكل صف متكامل ثنائي الأبعاد. وبإمكان آلة تصوير بهذه المواصفات عكس صورة أشياء يبلغ عرضها بعض المليمترات من على بعد متر واحد تقريباً. يتيح صف الهوائيات هذا التقاط 30 صورة بالثانية، كما هو الأمر مع آلات التصوير الفيديوية التقليدية وتكون النتيجة هي الحصول على صورة متحركة للعالم المحيط بالموجات المليمترية.

ويمكن بواسطة آلات التصوير المليمترية كشف أشياء معدنية مثل الخناجر أو المسدسات تكون مخبأة داخل الملابس وملامسة للجسم. كما انه يمكن تحديد المادة التي صنعت منها هذه الأشياء إذا ما عرفت حرارتها عن طريق تصنيف مستوى لمعان الصورة المعكوسة. ومعرفة حرارة الأشياء من الأمور السهلة نسبياً إذا ما كانت الأشياء موضوعة قرب الجسم، حيث أن نسبة اللمعان تتبدل حسب تبدل الحرارة، وحرارة الجسم تكون معروفة، وبالتالي فان تحليل الصورة المعكوسة على آلة التصوير تتيح تقدير الحرارة.

وهذه التقنية تسمح بكشف المواد البلورية المخبأة بسهولة، مثل

بعض أنواع المخدرات أو مثل السكر. إلا أنه ما يزال يصعب التمييز بين الأنواع المختلفة من هذه المواد.

وتقوم بعض الشركات بتطوير برامج كمبيوترية لمسح الصور المأخوذة بواسطة آلة التصوير الميليمترية وإنذار المراقبين في حال اكتشاف أشياء ممنوعة. والطريقة الوحيدة التي يمكن عن طريقها «خداع» البرنامج ربما تكون بإخفاء الأشياء داخل جسم من يتولى تهريبها. واستكشاف ما في داخل الجسم يتطلب استعمال معدات قادرة على بث وتحليل الموجات الصغرية.

الأجهزة المحللة للموجات الصغرية

إذا كان التقاط الصور بالموجات الميليمترية يتطلب استعمال آلات تصوير خاصة، فان تحليل الموجات الصغرية (Microwaves) يحتاج إلى رادارات خاصة تبث هذه الموجات وتحلل انعكاساتها، تماماً كما هو الأمر مع الرادارات التقليدية التي تتولى تغطية نطاق جوي معين بموجات، ثم تُعالج هذه الموجات ومن الأمثلة على هذه التطبيقات قيام مختبر لورانس ليفرمور الوطني (Lawrence Livermore National Laboratory) في ولاية كاليفورنيا الأميركية بتطوير جهازي رادار صغيرين لبث هذه الموجات والتقاط انعكاساتها المرتدة.

ويتم استعمال الرادارين بأن يبث كل منهما موجة صغرية على الشيء المطلوب مراقبته ويكون نطاق هذه الموجة الصغرية بضعة

أمتار، ثم تحلل انعكاسات البث. ويمكن وضع «مخطط راداري» كامل للشيء المطلوب مراقبته باستعمال الرادارين ثم دمج إشعاعاتهما مع ضبط قياساتها وفق مواصفات الشيء المطلوب تغطيته.

وتتيح هذه الرادارات الصغيرة الاستغناء عن عمليات التفتيش «اليدوية» التي يخضع لها المسافرون في المطارات، أو من يريد الدخول إلى بعض الدوائر الحكومية. كما انه يمكن استعمالها في عمليات التجسس والمراقبة، وذلك بالنظر إلى أن الموجات الصغرية تخترق الجدران والأبواب بسهولة. ولا تتعدى هذه المعدات الرادارية حجم قطعة الصابون، وعملية تجميعها زهيدة التكاليف. إلا أن البرامج الكمبيوترية لتحليل انعكاسات هذه الموجات معقدة وباهظة الثمن. وينتظر أن تنتشر مثل هذه الأجهزة بكثافة خلال العقد الأول من القرن الحادي والعشرين.

استعمال الموجات اللاسلكية لكشف الأشياء المعدنية: وعلى خط متواز مع تحليل الموجات الصغرية ابتكرت شركة رايثون (Raytheon) المتخصصة في الالكترونيات العسكرية طريقة جديدة للكشف عن الأشياء المعدنية. والفكرة هي أن يتم بث موجات لاسلكية (Radio Waves) يبلغ طولها بضعة أمتار، بحيث أن هذه الموجات تحرك الإلكترونيات في المعادن وتثيرها. وكثافة ومدة الاشعاع المعكوس مرتبطة بحجم وشكل الشيء الممسوح، بحيث يمكن معرفة ما هو هذا

الشيء إستناداً إلى معطيات هذه الإشعاعات المرتدة. وتخطط رايثون لصنع جهاز كاشف يبث الموجات اللاسلكية ويلتقط الموجة المرتدة. ومن بعد ذلك يتم إرسال هذه الموجة إلى قاعدة بيانات تتضمن «المواصفات اللاسلكية» للأشياء المعدنية المستهدفة (الخناجر، المسدسات إلخ...).

وما تزال الفكرة في مراحلها الأولى ولم يتضح بعد مدى إمكانية تحقيقها بصورة عملية وناجحة (ذلك في أول 1999).

أنظمة الشم الالكترونية

من المعروف أن كل إنسان يتميز عن غيره بمجموعة كاملة من الخصائص البيولوجية مثل البصمات ومخطط المورثات وغيرها. ولقد تمكن العلم من تصنيف بعض هذه الخصائص وتحديد هوية كل شخص بالاستناد إلى هذه الخصائص.

وبات بالامكان تصنيف الناس إستناداً إلى الروائح المنبعثة من أجسادهم، وذلك بواسطة «أنظمة شم الكترونية».

الروائح وتصنيفها الكترونياً: من المعروف أن جسم الانسان يفرز مئات المواد الكيميائية التي تحمل معها روائح متميزة (من أصل ألوف الروائح التي يفرزها الجسد) ولا يستطيع أنف الانسان التمييز بين معظم هذه الروائح (على عكس الكلب الذي يستطيع التعرف إلى صاحب الروائح بعد ثلاث سنوات) وإنما يمكن تصنيفها إستناداً إلى

الطبيعة الكيميائية لتكوينها.

ويعود تطوير «الأنوف الالكترونية» أو «الأنوف الاصطناعية» إلى السبعينات، والرائد الأبرز الذي قام بتطوير النماذج الأولى لهذه الأنوف هو العالم البريطاني جورج دود (Georges Dodd).

والأنوف الاصطناعية تتضمن مجموعات من 12 مستشعراً لالتقاط الروائح (أنف الإنسان يحتوي على نحو 10,000 مستشعر). وكل مستشعر مزود ببعض المواد البوليميرية (Polymers)، وتكون كل مادة قادرة على امتصاص مواد كيميائية عضوية معينة، وموصلة جيدة للتيار الكهربائي. ويؤدي إمتصاص الروائح إلى تبدل في نسبة التوصيل الكهربائي، وهو ما يطلق إشارة كهربائية معينة. ويكون مخطط الاشارات الكهربائية المختلفة المنبعثة من جميع المستشعرات هو «البصمة» المميزة الخاصة لكل رائحة. ويتم التعرف إلى هذه الرائحة عن طريق مقارنة مخططها الالكتروني مع مخططات الكترونية تكون مميزاتها مخزنة في قاعدة بيانات خاصة.

ولقد تم صنع بعض «الأنوف الاصطناعية» كما أن بعض دوائر الشرطة في عدد من البلدان الغربية (وخاصة في أوروبا) تحفظ قواعد بيانات لروائح بشرية. إلا أن نسبة اعتمادية (reliability)تلك الأجهزة لم تبلغ حتى الآن درجة من الدقة تكفي لاعتمادها بطريقة موثوقة ومن دون خطر ارتكاب هفوات، وذلك بالنظر إلى الدقة

الشديدة للمستشعرات حيث أن أي تغيير طفيف على التركيبة الكيميائية للروائح يكفي لإعطاء نتائج معكوسة لما هو مطلوب، دون أن ننسى صعوبة تصنيف الروائح.

هذا، ولا تقتصر فوائد تطوير أنظمة للشم الالكتروني على علم الاجرام أو المخابرات وإنما يمكن كذلك أن تشمل الطب وتسمح بتحقيق تحسن كبير في تشخيص الأمراض. والسبب في ذلك هو أن لكل مرض رائحته الخاصة، وأن تصنيف هذه الروائح ومقارنتها مع الروائح المنبعثة من جسم المريض تسمح بتحديد نوع المرض.

وقام البروفسور جورج دود، بالتعاون مع البروفسور جون باركر (John Parker) من جامعة كامبريدج (Cambridge University) بتطوير أنف الكتروني يتيح التمييز بين هذه الروائح، ومع إمكان إرسال نتائج التحليلات بواسطة الخطوط الهاتفية. والأنف الالكتروني هو بحجم الشريحة الالكترونية، إذ يضعها المريض في ميكروفون جهازه الهاتفي ويتنفس فيه عند الاتصال بالطبيب الذي يتلقى النتيجة على مرقاب جهازه الكمبيوتري الموصول بالخط الهاتفي، فيتمكن إذ ذاك من تحديد نوع المرض دون الاضطرار إلى عيادة المريض شخصياً.

ونشير أيضاً إلى أن هذه التقنية يمكن أن تستغل أيضاً لمعرفة ما إذا كان شخص ما يقول الحقيقة أو يكذب، ويمكن الاستفادة منها

لغايات التجسس، وذلك للتعرف إلى الحالة الطبية والنفسية للمتفاوض في حال تمكن الطرف المفاوض المقابل من زرع أنف الكتروني في الجهاز الهاتفي المستعمل لاجراء المحادثات.

بعض أنماط التنصت والتجسس التي تعتمد الأجهزة المنزلية المعتادة

ستائر التهوئة أو المرايا باتجاه واحد: يمكن تركيب آلة تصوير فيديوية عادية خلف ستائر التهوية، وترسل الصور الملتقطة بواسطة جهاز «ناقل الفيديو» (Video Sender) على شكل موجات كهرومغنطيسية يمكن أن يستقبلها جهاز تلفزيون عادي على بعد بضع مئات من الأمتار.

جهاز التلفزيون: تولد الأجهزة التلفزيونية إشارة كهرومغناطيسية بمكن التقاطها لاعادة تكوين الصورة الظاهرة على الشاشة بواسطة معدات خاصة يستطيع خبير الكتروني صنعها من المكونات المناسبة التي يمكن شراءها من متاجر متخصصة. ومعدات الكشف هذه يمكن أن تستعمل للتعرف على الصور التي تبث على شاشات التلفزيون أو أجهزة الكمبيوتر أو حتى على أنظمة الفيديو عند مدخل البنايات.

مقابس الهاتف: يمكن تسجيل المكالمات بواسطة آلة تسجيل يتم تشغيلها على الموجات الصوتية مباشرة ولا يتعدى حجمها حجم علبة

السجائر وهذه المسجلات يتم ربطها بمقابس الهاتف.

مسجل للأشرطة:يمكن تسجيل رسائل الفاكس بواسطة مسجل صوتي بالأشرطة ذات نسبة دقة عالية جداً، ويمكن بث الاشارات بواسطة ناقل للموجات مركب على الوصلة الهاتفية، ليتم استقبالها في ما بعد على جهاز خاص.

النوافذ:ان التكلم داخل الغرف يولد موجات صوتية تتسبب باهتزاز زجاج النوافذ، ويمكن قياس هذه الاهتزازات وتحويلها إلى أصوات أو كلمات مفهومة عن طريق بث شعاع ليزري على النافذة. إلا أن هذه الطريقة دقيقة وصعبة جداً، خاصة أن الرياح والأمطار تتسبب أيضاً بالاهتزازات وبالتالي تستطيع أن تغطي على الاشارات الصوتية.

استعمال آلات التصوير:يمكن اخفاء الات التصوير المصغرة في مجموعة واسعة من الأجهزة مثل الكمبيوترات الشخصية أو الحقائب أو التلفزيونات المنزلية. وهو ما يسمح باستعمالها من دون أن يشعر أحد بوجودها.

المكاتب:يمكن اخفاء ميكروفونات صغيرة ومعدات لنقل الموجات في أية قطعة من معدات المكاتب العادية مثل أجهزة الهاتف أو الآلات الحاسبة أو الأقلام والمنافض...

أما في ما يتعلق بمحاربة أعمال التنصت التي تتم عبر أنظمة أكثر

تعقيداً كتلك التي استعرضناها أعلاه، فانها تتم عن طريق التقصي حول وجود معدات الكترونية تبث إشارات كهربائية، وفحص هذه المعدات للتأكد من الأمر بالنسبة للمستعملين. وهناك أنظمة كاشفة تستطيع كشف جميع تلك المعدات باستقبال إشاراتها اللاسلكية وفي ما يختص بالمعدات الالكترونية غير العاملة عند إجراء أعمال البحث، يتم كشفها عن طريق إرسال موجات لاسلكية من شأنها أن تجعل المكونات الالكترونية (الترانزستورات إلخ.) للأجهزة تبث موجة مضاعفة، تكشف عن وجودها.

الفصل التاسع:

أنظمة تشفير بيانات الاتصالات

يمكن القول أن سعي الانسان إلى جعل الرسائل التي يبعثها سرية لا يتمكن من قراءتها غير الشخص المرسلة إليه الرسالة، يعود تقريباً إلى الوقت الذي بدأ فيه بنو البشر بتبادلون الرسائل. كذلك فإن المساعي لفك الرموز المستعملة لجعل الرسائل سرية، أو بكلام آخر لفك الشيفرات تعود أيضاً إلى الوقت الذي بوشر فيه تبادل الرسائل السرية. وروايات التاريخ القديم والحديث مليئة بالقصص التي تدور حول قضايا تجسس كان محورها تشفير المعلومات والمساعي الرامية إلى فك رموز التشفير.

وكان من الطبيعي أن تلعب أنظمة التشفير دوراً بارزاً في وسائل الاتصال الحديثة التي تعتمد على الخطوط السلكية واللاسلكية، وقد اتسع نطاق مستعملي أنظمة التشفير ليشمل الشركات التجارية والصناعية، وليس فقط الدوائر الحكومية. كذلك تتزايد مساعي السلطات العامة لفك أنظمة التشفير،

خصوصاً وإن عصابات الإجرام المنظم باتت من بين أكثر من يعتمد على الشيفرة لضمان سرية إتصالاتها. ولقد بات الكمبيوتر يلعب اليوم دوراً أساسياً كوسيلة للاتصالات بواسطة الخطوط الهاتفية وأجهزة الموديم. وينتظر أن تتزايد أهمية هذا الدور خلال السنوات المقبلة مع بزوغ عصر ما يعرف «بجادة المعلومات»(information highway).

ولقد ارتدت أنظمة التشفير دوراً أساسياً في السنوات الأخيرة مع الانتشار الواسع لشبكات الاتصالات الكمبيوترية، وحاجة الاطزاف الدولية (من اقتصادية، وسياسية، وعسكرية..). التي تتولى تأمين الاتصالات إلى ضمان سريتها وتحصينها ضد مساعي من يتطلع إلى اختراقها والاطلاع على مضمونها.

وكانت الاتصالات الكمبيوترية تعتمد في الاساس وبصورة خاصة على كلمات للسر لضمان سريتها، بيد أنه كان بإمكان القراصنة التغلغل إلى هذه الاتصالات عن طريق الحصول على كلمة السر بطريقة أو بأخرى. وعادة عن طريق نسخ إشارة التعريف عن المستعمل. ثم السعي لايجاد كلمة السر في الرسالة. وكل هذا بواسطة برنامج خاص يتولى إرسال المعلومات إلى «القرصان» الذي يستطيع «تجربة» كلمات السر التي يتلقاها بهذه الطريقة. وعلى الرغم من وجود برامج أمنية للحؤول دون حصول

القـراصنة على كلمـات السـر، فـإن الخـبـراء أنفسـهم يعتـرفـون بإستـحالة القضاء على القرصنة؛ جدير ذكره انه توجد أنظمة لبث الرســائل عـبـر شـبكة «انـتـرنت» دون ذكـر اسم المرسل، ويـتم ذلك بإرسـال هذه الرسـائل إلى مـركز إعـادة إرسـال هو كناية عن مزود (server) كمبيوتري يتولى «نزع» إشـارة التعريف عن الرسـالة قبل إعـادة إرسـالـهـا دون ذكـر إشـارة التـعـريف هذه. وتعـتـمـد بعض الشـركات المتخصصة هذه الطريقة للاتصـالات الهـاتفية الصـوتية أيضاً، حيث يتم توجيه الاتصـالات الهاتفية إلى مركز إعـادة توجيه يتولى إعادة إرسالها إلى الوجهة المطلوبة وهذا يحول دون إمكانية تعقب المسار الدقيق للإتصال الهاتفي.

وتعـتـمـد الاتصـالات الكمـبـيوترية اليوم إعتمـاداً مكثفـاً على برامج التشفير لتأمين سـرية الاتصـالات. وهناك فئتان من برامج التشفير: الفئة التقليدية التي تقضي باعتماد برامج تشفير خاصة بكل مستعمل، ومشكلة هذه الطريقة هي إضطرار طرفي الاتصـال إلى اعتمـاد نفس برنامج التشـفير، مع إمكانية سـرقة الشـيفـرة أو فكها من قبل القراصنة بسـهولة ويسر. والفئة الثانية المعتمدة اليوم بصـورة مكثفـة تسـتـعـمل برامج تشـفير «عـمومـية» (Public)، مـع برنامج خـاص لفك التشـفير. ومع هذه الطريقة، يختـار المسـتـعمل برنامج تشـفير عـمومي مـرتبط ببرنامج شـخصي لفك الشـيفرة

بحيث يرسل برنامج التشفير العمومي إلى الجهة التي يطلب منها بيانات معينة، فتقوم هذه الجهة بتشفير الرسالة وترسلها إلى وجهتها. ويتم فك الشيفرة بواسطة الشيفرة الخاصة. والميزة البارزة في هذه الطريقة هي أن التقاط الشيفرة العمومية من قبل القراصنة لن يفيدهم بشيء طالما أنه لا يمكن فكها إلا بواسطة البرنامج الخاص. وهذا البرنامج الخاص موجود عند صاحبه وحده. ومن الواضح أن عملية الحصول على شيفرة موجودة عند شخص واحد أصعب من عملية الحصول على شيفرة موجودة عند عدة أشخاص. ونشير هنا إلى وجود برامج تتيح تشفير الاتصالات بصورة لا تثير الشبهات، أو بكلام آخر لجعل الشيفرة تبدو على شكل رسالة عادية. مثلاً، تشفير رسالة تجارية على شكل تبدو وكأنها رسالة شخصية، بحيث أن القرصان لن ينتبه إلى أن ثمة رسالة تجارية سرية يجري تبادلها أو يتصور أن الأمر يتعلق بمجرد أمور شخصية لا أهمية لها لغير أصحابها.

وهناك طريقة أخرى لضمان سرية الاتصالات الكمبيوترية وهي اعتماد «التواقيع الالكترونية» الخاصة بكل مستعمل، والتي هي كناية عن شيفرة تصدر عن الكمبيوتر الخاص بهذا المستعمل وتجعل من يتلقى الرسالة يتأكد من مصدرها الحقيقي.

وكان من الطبيعي أن يشكل موضوع أنظمة التشفير إحدى

نقاط الارتكاز لمجلس الأمن القومي في الولايات المتحدة، وكذلك للهيئات المخابراتية في معظم بلدان العالم، وذلك من ناحيتي تطوير شيفرات معقدة لا يمكن اختراقها لحساب الدوائر الحكومية، أو لفك شيفرات الجهات المعادية.

ولقد فرضت وكالة الامن القومي الاميركية قيوداً صارمة على انتاج برامج التشفير الاميركية، وذلك لجهة فرض حد أقصى لطول الشيفرة (من ناحية قياسها بالبتات) (Bits) مع فرض وضع «مفاتيح» الكترونية في برامج التشفير تسمح للوكالة بفك الشيفرة عند الضرورة.

وقد وضعت عدة بلدان أخرى، (ومنها فرنسا بصورة خاصة) قيوداً مماثلة، إلا أن ثمة دولٍ لم تضع قيود من هذا النوع كما سبق وأشرنا إلى الأمر وهذا ما يجعل برامجها التشفيرية أكثر جاذبية للزبائن، بالنظر إلى صعوبة خرقها من الناحية المبدئية (مع العلم بأن أميركا والدول الأخرى تبرر فرضها للقيود «بضرورة محاربة الاجرام والارهاب الدوليين». وهذا يعني ضرورة الحصول على طريقة تتيح التجسس على بيانات البلدان الأخرى بكلام صريح..).

في مطلق الأحوال، حصل أكثر من مرة أن مبرمجين مستقلين تمكنوا من فك أنظمة التشفير وتحصين التشفير الحكومية

الأميركية.

كذلك، فان اصرار الوكالات المخابراتية، (وخصوصاً في الولايات المتحدة) على فرض قيود تقنية على تصميم برامج التشفير وعلى أن تكون مطلعة على مفاتيح التشفير العمومية قد يشكل دليلاً على أن الأنظمة الكمبيوترية المعقدة التي تستعملها هذه الوكالات عاجزة عن فك جميع الشيفرات، والدليل الآخر على عجز الأنظمة الكمبيوترية هو سعي هذه الوكالات دائماً على الاتصال مباشرة بشركات البرامج والمعدات للاطلاع على شيفرات البرامج الكمبيوترية التي تنتجها هذه الشركات، وخصوصاً البرامج التي يتم تصديرها إلى الخارج، وأمر الضغوطات التي تمارس على الشركات بات معروفاً جيداً. ولا تقتصر هذه الضغوطات على شركات بلد الوكالة المخابراتية، بل تشمل شركات من بلدان أخرى، ويعطي افتضاح حصول وكالة الأمن القومي الاميركية على أسرار أنظمة التشفير التي كانت تستعملها السفارات الايرانية من الشركة السويسرية كريبتو مثالاً جيداً عل ذلك (يُراجع بهذا الخصوص الملحق الخاص بهذه القضية)..

خلاصة القول أن أنظمة التشفير سوف تأخذ أهمية متزايدة في السنوات المقبلة، خاصة وأن تصميمات وحدات المعالجة الكمبيوترية سوف تتضمن تسهيلات تشفيرية في المستقبل ستسعى وكالات المخابرات دائماً للاطلاع على هذه الأسرار، إلا أن مهمتها لن تكون سهلة...

ملحق

شركة سويسرية لأنظمة التشفير تتعرض لحملة تشكيك مركزة حول مسألة حيادها

تُعتبر أعمال المتاجرة بالمعدات والبرامج التي تستعمل لتشفير البيانات من أدق الأمور وأخطرها وأكثرها حساسية بالنظر إلى مدى علاقة هذه المنتجات بمسائل الأمن القومي، إذ تستعمل للحفاظ على سرية الاتصالات والمعلومات الخاصة بكل دولة، وهذا الأمر كان يفسر إلى حد بعيد نجاح شركة كريبتو (Crypto) في هذا المجال فكريبتو هي شركة متخصصة في انتاج أنظمة للتشفير تستعمل في الاتصالات على مختلف أنواعها من اتصالات هاتفية أو بالفاكس أو البريد الالكتروني.

ولقد قام بتأسيس هذه الشركة المواطن الأسوجي من أصل روسي بوريس هاجلين (Boris Hagelin)، ومقر الشركة في سويسرا أي أن مؤسس الشركة هاجلين هو مواطن دولة حيادية (أسوج) وقد إختار دولة حيادية أخرى (سويسرا) لتكون مقر شركته، وفي ذلك ما كان يضمن مبدئياً أن شركة نفسها سوف تلتزم الحياد في أعمالها ولن تكشف عن أسرار الأجهزة التي تبيعها، أياً كان الزبائن.

ويعتبر العديدون أن هاجلين هو أحد أبرز الخبراء في التشفير، وكان قد اخترع جهازاً متطوراً للتشفير استعمله الجيش الأميركي خلال الحرب الكونية الثانية.

ولقد ازدهرت اعمال كريبتو بعد الحرب الكونية الثانية وحتى التسعينات ويُعتقد بأن أكثر من 130 دولة ومنظمة دولية قد اشترت معدات من انتاجها ومن بينها حاضرة الفاتيكان ومنظمة الأمم المتحدة وإيران ومصر وغيرها .ومن أبرز مزايا معدات كريبتو انها تعتمد على معايير الشركة الخاصة، وبالتالي يفترض أن لا يتمكن أحد من الاطلاع على أسرارها وبشكل خاص الأحلاف العسكرية مثل حلف شمالي الأطلسي «الناتو».

ولا يقتصر عمل كريبتو على انتاج معداتها وبرامجها فقط، بل انه يشمل أيضاً تدريب مستعملي هذه المنتجات على استعمالها، حيث تنظم دورات تدريبية بثمانية لغات في مقر الشركة ويحضر هذه الدورات نحو 800 شخص يأتون من مختلف أنحاء العالم.

ومن الطبيعي أن يكون مقر كريبتو هدفاً مميزاً لممارسة أعمال التجسس إلا أن كريبتو تحرص حرصاً شديداً على الحفاظ على طابع سرية أعمالها، وذلك من أجل تلافي هذا الأمر فالشركة كانت ترفض الكشف عن قيمة أعمالها وعن أسماء زبائنها. إلا أن

هذا الأمر لم يمنع حصول عدة فضائح مرتبطة بالشركة.

فلقد كشف كتاب وضعه الضابط المخابراتي البريطاني المتقاعد بيتر رايت (Peter Wright) بأن دائرة المخابرات البريطانية تمكنت من فك أنظمة تشفير السفارات المصرية خلال حرب السويس سنة 1956، وكانت مصر تعتمد فيها على أجهزة كريبتو.

وفي 1992 حصلت فضيحة أهم من ذلك بكثير وهي أن الموظف السويسري لدى الشركة هانس بوهلير (Hans Buhler) أعتقل أثناء قيامه بأعماله لحساب كريبتو في الجمهورية الاسلامية الايرانية بتهمة ممارسة التجسس لمصلحة وكالة الأمن القومي وبعد أن تم الافراج عنه على أثر مفاوضات معقدة لسنا هنا بصدد بحثها، عاد إلى سويسرا ورفع دعوى على كريبتو متهماً إياها بأنها كانت تتعامل بالفعل مع الوكالة الأميركية من وراء ظهره وانه ذهب ضحية هذا التعامل. ولقد انتهت القضية بتسوية التزم بوهلير الصمت بموجبها، إلا أن القضية لم تنته عند هذا الحد، حيث عاد صحافيون سويسريون وأكدوا صحة ادعاءات بوهلير في حين أكد خبير أميركي بأن كريبيتو كانت تتعامل في الواقع مع المخابرات الالمانية وليس الاميركية..

والحقيقة أن هذه الاتهامات قد يكون بولغ فيها بمعنى أن شركة كريبتو نفسها ربما لم تكن هي المذنبة،وإنما قد يكون

عـاملون لديهـا تورطوا دون علم الادارة غـيـر أن الشـيء الأكـيـد والثـابت هو انه لا يمكن لأية دولة أن تثق بطرف خـارجي عندمـا يتعلق الأمـر بمسـائل الأمن القـومـي، وبالتـالـي فـان المطلوب هو أن يكون لكل دولة وبشكل خـاص لكل دولة عـربيـة، نظامـهـا الأمني والمخـابراتي الخـاص بهـا مع اسـتـعمـال تقنيين وخـبـراء يحـملون جنسية البلد نفسه.

الفصل العاشر:

اعتماد العسكريين على التقنيات المعلوماتية المدنية

خلافاً لما يعتقده العديدون، فإن المستوى التكنولوجي المعلوماتي في جيوش البلدان الغربية لا يتفوق على ذلك الخاص بالقطاعات المدنية المختلفة، بل أن مستوى الأنظمة المدنية يعتبر أعلى من المستوى العسكري في حالات كثيرة...

ولعل الدليل الأبرز على هذا الأمر أن معظم الجيوش في البلدان الغربية باتت تعتمد على أنظمة معلوماتية مدنية، وذلك لسببين:

الأول يعود إلى تفوق هذه الأنظمة في حالات عديدة، وهو ما يغني عن الحاجة لتطوير نظام عسكري خاص، والثاني هو ذات طابع مالي بحت حيث أن الأنظمة المدنية أقل كلفة من الأنظمة العسكرية الخاصة، بطبيعة الحال...

بيد أن العديد من الخبراء العسكريين الغربيين باتوا يتخوفون

من عواقب هذه الظاهرة، ذلك أن الأنظمة المعلوماتية المدنية غير مصممة بطريقة تجعلها ملائمة لشروط العمليات العسكرية، خاصة من الناحية الأمنية ومن ناحية اعتمادية التشغيل، وفي هذا المجال أفادت بعض المصادر بأن سفينة تابعة لسلاح البحر الأميركي وجدت نفسها متوقفة في عرض البحار في 1998بعد أن تعطلت 90٪ من أجهزتها، وذلك بسبب خلل أصاب النظام التشغيلي الكمبيوتري الذي كان يتحكم بهذه الأجهزة وهو من نوع وندوز ان تي (Windows NT). من ناحية مقابلة، تعاني وكالات المخابرات الأميركية من صعوبة لاجتذاب خبراء الكمبيوتر ليعلموا لديها وذلك بسبب تدني مستوى الرواتب في هذه الوكالات بالمقارنة مع رواتب شركات القطاع الخاص.

ولقد اطلقت وكالة المخابرات المركزية الأميركية (سي أي آي) برنامجاً طموحاً سنة 1998 لتوظيف اخصائيين في علوم الكمبيوتر، ووضعت موقعاً على شبكة الانترنت لهذه الغاية، كما تقوم الوكالة بحملات توظيف مكثفة في الصحف والمجلات الاقتصادية والعسكرية، وكذلك بين صفوف الجامعيين والعسكريين والهدف هو توظيف عدد قياسي من خبراء الكمبيوتر (ولم يتم الكشف عن هذا العدد بالنظر إلى الطبيعة السرية لعمل الوكالة) بين 1998 و2005.

وتقول ناطقة باسم وكالة المخابرات المركزية الأميركية بأن الوكالة تتطلع حالياً إلى توظيف مهندسين ومبرمجين معلوماتيين يستطيعون التعاطي مع أنظمة تشغيلية كمبيوترية متعددة ومع برامج تطبيقية من فئات متنوعة.

ولقد ذكرت مقالة صحفية نشرتها جريدة نيويورك تايمس(New York Times) بأن وكالة سي أي آي باتت تجد صعوبة في ارسال عملاء لها يستعملون جوازات سفر مزورة للدخول إلى بعض البلدان المعادية للولايات المتحدة والخروج منها، وذلك بالنظر إلى أن انتشار الشبكات الكمبيوترية سهلت على دوائر الأمن العام في معظم دول العالم الاتصال بسفاراتها وقنصلياتها للتأكد من صحة جوازات السفر أو سمات الدخول، وبالتالي فإن الخبراء الكمبيوتريين سوف يسهلون على الوكالة مهمة التسرب إلى الأنظمة الكمبيوترية الخاصة بالدول الأجنبية والاطلاع على البيانات المخزنة فيها، مما يسمح بصنع مستندات رسمية مزورة على قدر عالٍ من الشبه مع المستندات الحقيقية... وليس هذا سوى مثال واحد للحالات التي تبرز فيها حاجة الوكالة إلى خبراء الكمبيوتر...

وفي ما يتعلق بوكالة الامن القومي الأميركية، فإن المشكلة البارزة لديها تكمن في كيفية المحافظة على الخبراء في العلوم

الكمبيوترية والرياضية لديها والحؤول دون تركهم لها وتوجههم إلى شركات القطاع الخاص.

ولقد أفادت معلومات صحفية بأن هذه الوكالة تعاني في الوقت الحاضر (سنة 1999) من «نزيف حاد للأدمغة» حيث تركها العديد من الخبراء للعمل في شركات خاصة.

والجدير ذكره أن وكالة الأمن القومي كانت حققت نجاحات هامة في الثمانينات وأوائل التسعينات لاجتذاب مجموعة متميزة من خبراء الكمبيوتر، هو ما جعل منها أكبر جهة تشغل أخصائيين في الرياضيات بالولايات المتحدة (في1999) وهي تعمل على توظيف أكثر من 100 حاملاً لشهادة بي ايتش دي (PHD) في العلوم الرياضية بين 1998 و2001. وافتتحت الوكالة موقعاً لها مخصصاً للتوظيف، وافادت بأن 20٪ من موظفيها الجدد قد أرسلوا عروضهم عن طريق هذا الموقع. كما أن لدى الوكالة عدة برامج تهدف إلى اجتذاب طلاب وأساتذة الجامعات والمعاهد العليا.

وإذا كانت وكالة الأمن القومي أكثر الجهات براعة في مجال العلوم والتطبيقات الرياضيات في أميركا وربما في العالم بالوقت الحاضر، فإنها بدأت تشكو منذ أواسط التسعينات من أن الفارق في مستوى هذه العلوم بينها وبين الشركات التكنولوجية

من القطاع الخاص الأميركي (والغربي بصورة عامة) آخذ في التقلص، وذلك على الرغم من أن الشركات التكنولوجية لا تركز على العلوم الرياضية البحتة بقدر ما تركز على التطبيقات التكنولوجية للعلوم الرياضية بينما تحتاج وكالة أن أس آي إلى خبراء في الرياضيات يقومون بتطوير خوارزميات معقدة لأنظمة التشفير.

هذا، وتركز مدارس ومعاهد تدريب الجواسيس الأميركيين مناهجها التدريبية والتعليمية حالياً على تلقين الطلاب علوم الكمبيوتر وكيفية التعامل مع شبكات الاتصالات، وعلى رأسها شبكة الانترنت، مع التدريب على كيفية فرز البيانات المنشورة على مواقع الانترنت وانتقاء المجدية لنشاط المخابرات من بينها، خصوصاً وأن مهمة جمع المعلومات باتت تعتمد بصورة متزايدة على مصادر المعلومات غير السرية.

والواقع أن هناك العديد ممن يؤكدون بأن معظم الذين ينخرطون في هذه الوكالات الأميركية هم خبراء من مستويات متوسطة لم يجدوا وظيفة مرموقة في الشركات الخاصة، وهو ما اضطرهم إلى التوجه للعمل في القطاع العام... ومن هنا ندرك السبب في تدني المستوى العلمي لهذه الوكالات في المرحلة الراهنة.

ملحق

اعتماد شركات صناعة الطائرات المدنية على تقنيات الكترونية عسكرية

في مقابل اعتماد العسكريين على التكنولوجيا المدنية بصورة متزايدة فإن الشركات التكنولوجية المدنية تعتمد أيضاً على التكنولوجيا العسكرية، وخصوصاً شركات صناعة الطائرات، حيث من المعروف أن اسقاط الطائرات المدنية التي تحمل رؤساء أو مسؤولي الدول يمكن أن يشكل جزءاً أساسياً للتخطيط للحروب، والمعروف مثلاً أن مجازر رواندا كانت قد بدأت على أثر اسقاط طائرة رئيسي رواندا وبوروندي في السادس من نيسان (ابريل) 1994، وتطلب عدة شركات طيران من صانعي الطائرات المدنية تزويد طائراتها بأنظمة حماية وتشويش الكتروني مشابهة لتلك المستعملة في الطائرات المقاتلة: وقد ذكرت مصادر صحافية فرنسية في هذا المجال بأن مجوعة ايرباص (Airbus) الأوروبية تعاقدت مع شركة لوكهيد مارتن (Lockheed - Martin) الأميركية لتطور لها هذه الأخيرة بعض أنظمة الحماية.

والمعروف أن لوكهيد ـ مارتن شديدة الارتباط

بوكالات المخابرات الاميركية وهي صنعت عدة طائرات أو أقمار اصطناعية مخصصة لمهمات التجسس، ومن هنا فإنه قد لا يكون من الصعب تزويد طائرات ايرباص بأنظمة تجسس وتنصت أميركية، وخصوصاً في الطائرات المخصصة لمسؤولي الدول المناهضة الأميركية والذين يختارون طائرات ايرباص بدل طائرات بوينغ على أساس أنها أوروبية وليست أميركية، علماً أن طائرات المسؤولين هي التي تم تزويدها بأنظمة الحماية بالأولوية....

الفصل الحادي عشر:

النشاط المخابراتي اليهودي

صدرت عدة كتب ودراسات ومقالات حول النشاط المخابراتي اليهودي ضد البلدان العربية ولا ضرورة لتكرارها.

والمهم في هذا البحث هو أن الكيان اليهودي يركز على تطوير التكنولوجيات الأمنية والمعلوماتية مع وضع عدة برامج ومعدات للأمن المعلوماتي، ولتشفير البيانات، أو لفك الشيفرات (راجع بهذا الصدد ما أوردناه في كتابنا «حرب الكمبيوتر في فلسطين»).

وأفادت عدة تقارير بأن اليهود نجحوا في زرع معدات للتنصت والمراقبة في العديد من شبكات الاتصالات وأجهزة الكمبيوتر بالعالم العربي، وخصوصاً في مناطق «الحكم الذاتي» الفلسطيني المحدود؛ كما يعتمد اليهود بصورة مكثفة على نفوذ الجماعات اليهودية المتفشية في معظم أنحاء العالم (يُراجع بهذا الخصوص كتابنا «أسرار اللوبي اليهودي في العالم»).

على أن اليهود يعتمدون أيضاً اعتماداً كاملاً على الولايات المتحدة

لتزودها بالمعلومات حول العالم العربي، وتم إبرام العديد من اتفاقات التعاون بين الكيان اليهودي والولايات المتحدة في جميع مجالات المخابرات من عسكرية وأمنية واقتصادية، كما أن الولايات المتحدة تفرض قيوداً صارمة على تصدير بعض فئات المعلومات المتعلقة بالكيان اليهودي، وذلك لكي لا يستفيد منها اعداء «إسرائيل»، ومن الأمثلة على ذلك منع تصدير صور فلسطين ذات نسبة الوضوح الدقيقة للغاية. التي يتم التقاطها بواسطة الأقمار الاصطناعية الاميركية التجارية ..ولقد أصيبت المخابرات اليهودية بنكسات عديدة في النصف الثاني من التسعينات، في حين تضاءلت نسبة النجاح في عملياتها على ما يبدو.

والأمر الأخطر بالنسبة إلى اليهود قد يكمن في قضية الجاسوس اليهودي الأميركي جوناثان بولارد (Jonathan Pollard) الذي اعتقل سنة 1985 بعد أن سرق أكثر أسرار المخابرات الأميركية حساسية وسربها إلى الكيان اليهودي، وقد حكم عليه بالسجن المؤبد؛ والمهم في هذه القضية هو أن الأميركيين رفضوا بإصرار منح العفو لهذا اليهودي وانكشف سر هذا الاصرار في بداية 1999 عندما سربت وكالة المخابرات المركزية الأميركية إلى مجلة «ذي نيو يوركر» (The New Yorker) خبراً يؤكد بأن خطورة أعمال بولارد هي أن الكيان اليهودي قام بتزويد الاتحاد السوفياتي السابق بالمعلومات التي كانت

ترده من بولارد، وذلك مقابل أن يسمح الحكم السوفياتي بشحن العلماء اليهود السوفيات إلى فلسطين المحتلة؛ وبالفعل تجاوب الاتحاد السوفياتي مع هذا المطلب «اليهودي» في الثمانينات وأول التسعينات، وهذا من الأسباب الرئيسية التي جعلت عدد العلماء والمهندسين يصل إلى مستويات قياسية بين اليهود في فلسطين..

المهم في الأمر أنه تبين للأميركيين بصورة آخذة في التوضح والتجلي على نحو متزايد أن «إسرائيل» لا يمكن أن تكون حليفاً استراتيجياً للولايات المتحدة وانها لا تتردد في الطعن بظهر أميركا والعبث بمصلحة الأمن القومي الأميركي عندما تقضي مصلحة اليهود بذلك. وهذا لا يعني أن الولايات ا المتحدة سوف تتحول من حليف وداعم لليهود إلى عدو لهم وصديق للبلدان العربية بين ليلة وضحاها، وإنما يعني أن التعاون الأميركي اليهودي في المجال المخابراتي بدأ يتقلص وأن الأميركيين لم يعودوا يثقون باليهود، وهذا لوحده يشكل مكسباً مهماً للبلدان العربية وعليها أن تسعى للاستفادة منه عن طريق التعاون مع الأطراف الأميركية المعادية لليهود (أو غير المتحمسة لهم على الأقل..) مع التشدد في رفض أي نوع من أنواع تطبيع العلاقات مع اليهود والتعامل معهم.

هذا، وسوف يسعى اليهود في السنوات القليلة المقبلة إلى توسيع نطاق نشاطهم المخابراتي في العالم العربي مع تكثيف جهودهم

لتجنيد العملاء لهم وزرع الشبكات العربية بمعدات التنصت، مع تخفيف اعتمادهم على الأميركيين.

ويجب أن تنصب الجهود الأمنية العربية على التصدي لهذه المساعي مع اعداد خطط هجومية مضادة.

ملحق

طريقة «إسرائيلية» لفك شيفرات البيانات الكمبيوترية

تركز الشركات الكمبيوترية «الاسرائيلية» كثيراً على تطوير تقنيات الأمن المعلوماتي لصد أعمال القرصنة ولمحاربة تفشي الفيروسات.

وفي هذا الإطار، إبتكر اختصاصيان «إسرائيليان» في علوم الرياضيات في 1996 طريقة لفك الشيفرات الكمبيوترية أياً كان طولها عن طريق الموجات الميليمترية، ولقد انطلق الخبيران في عملهما من اكتشاف لمركز أبحاث شركة بيلكور (Bellcore) للاتصالات، حيث تبين أن بث ميكرو موجات يمكن أن يؤثر بصورة طفيفة على محتويات بطاقة ذكية تكون موضوعة قرب مصدر البث، وهو ما يؤدي إلى حصول أخطاء في البيانات التي تتضمنها البطاقة.

وتقوم طريقة فك الشيفرة على إرسال نص معروف ليتم تشفيره بالطريقة العادية. وبعد ذلك يرسل النص نفسه بعد

تعريضه لموجات ميليمترية بغية تعديل محتويات بياناته بصورة طفيفة، وهو ما يؤدي بدوره إلى تعديل مواز في مفتاح التشفير. وتكرر العملية أكثر من مرة مع تعديل طريقة بث الموجات في كل مرة، وبعد ذلك تتم مقارنة الرسالة المشفرة بالصورة الصحيحة مع الرسائل الأخرى بواسطة برنامج كمبيوتري خاص .ويؤكد العالمان، «الاسرائيليان» بأن هذه الطريقة تسمح بالتعرف إلى كل مفتاح تشفير، وبالتالي إستعماله للاطلاع على البيانات التي تم تشفيرها بواسطة هذا المفتاح.

ولا يمكن في الوقت الحاضر (أول 1999) التأكد مما إذا كانت هذه الأقوال دقيقة آم مبالغ فيها، مع العلم أن نكسات المخابرات «الاسرائيلية» في أواخر التسعينات تؤكد بأن تقنيات هذه المخابرات ليست أبداً من النوع الذي لا يخطىء.

خاتمة

ليس القصد من هذا الكتاب هو بعث الذعر في النفوس عن طريق إظهار التفوق التقني في مجال جمع المعلومات لدى اليهود والولايات المتحدة، وإنما عدم ممارسة سياسة النعامة التي تخبىء رأسها في الرمال عند حصول الخطر، متوهمة بأن عدم مشاهدة الخطر يعني زواله... والواقع أن العرب ليسوا عاجزون في عالم المخابرات، بل إنهم حققوا عدة نجاحات ويملكون طاقات كبيرة في هذه المجالات ولم يتم استغلالها بالطريقة المناسبة دائماً في ظل غياب خطة واضحة للتصدي لليهود وفي تحديد أولويات الصراع.

ولا يتطلب البحث عن المعلومات الهامة التي تؤثر على الأمن القومي في الدول اعتماد وسائل سرية معقدة بالضرورة، بل يكفي في حالات كثيرة قراءة الصحف والاطلاع على البيانات المنشودة على مواقع الانترنت.

ومن الأمثلة ذات الدلالة التي تعكس هذا الواقع أن وكالة المخابرات المركزية الاميركية «سي أي آي» تحملت قسطاً وافراً من اللوم في سنه 1998 لأنها عجزت عن توقع اجراء الهند تجارب للتفجيرات النووية، وعند البحث تبين أن احدى المجلات الهندية الواسعة الانتشار

كانت قد أعلنت عن قرب اجراء هذه التجارب قبل حصولها بثلاثة أيام ولم يتنبه عملاء الوكالة في الهند إلى هذا المقال الذي كان يمكن الحصول عليه عند جميع باعة الصحف والمجلات في الهند. ويلخص أحد الخبراء الاميركيين في علوم المخابرات نظرية الاعتماد على المصادر المفتوحة غير السرية (open source intelligence) قائلاً أن: «إذا تم انفاق 20٪ من الميزانية المرصودة للمخابرات على البحث عن المعلومات في المصادر المفتوحة، يمكن الحصول على الأجوبة الشافية لـ 70٪ من تساؤلات المسؤولين عن المخابرات».

ويعني هذا بأن الشرط الأساسي للقيام بنشاط مخابراتي ناجح لا يقتصر على تطوير واستعمال أحدث التقنيات والحصول على جميع المعلومات وإنما يكمن أيضاً في معرفة كيفية فرزها واستغلالها، مع العلم بأن الحصول على المعلومات يمكن أن يتم بمجرد قراءة الصحف أو التنقل بين مواقع شبكة الانترنت، شرط معرفة ما هي المعلومات المطلوبة وأين يتم إيجادها... أي بمجرد استعمال منطق سليم وتفكير راجح... مع الاشارة هنا إلى أن الدول والحكومات ليست وحدها القادرة على اعتماد طريقة استقصاء المعلومات بواسطة المصادر المفتوحة، وإنما أيضاً شركات القطاع الخاص، علماً بأن هذه الشركات أخذت بالفعل تزيد نشاطها في المجالات المخابراتية المختلفة، وهي تستغل المعدات المطروحة في

الأسواق، فضلاً عن دراسة وتحليل المصادر المفتوحة بطبيعة الحال، وخصوصاً مواقع شبكة الانترنت.

خلاصة القول أن الشرط الأساسي لتحقيق التفوق في لقرن الحادي والعشرين ميلادي هو الحصول على المعلومات الأساسية، ومعرفة كيفية الاستفادة منها دون الاكتفاء بمجرد تجميعها، والاستفادة من المعلومات تتم عن طريق تحديد نظرية دقيقة حول كيفية تنفيذ المخططات السياسية والعسكرية والاقتصادية لتحقيق الاهداف القومية لكل أمة، وذلك بعد أن يكون قد تم تحديد هذه الأهداف بصورة واضحة.

أبرز المصادر:

● دوريات عربية:

- مجلة البناء.
- مجلة فلسطين الثورة.
- مطبوعات دار الصياد.
- جريدة الشرق.
- جريدة الديار.
- جريدة الكفاح العربي.

●دوريات أجنبية:

- مجلة أفياشن ويك (Aviation Week) الأميركية.
- مجلة جاينز ويكلي (Jane's Defense Weekly) البريطانية.
- مجلة لو بوان (Le Point) الفرنسية.
- مجلة لونوفيل أوبسيرفاتور (Le Nouvel Observateur) الفرنسية.
- مجلة بزنس ويك (Business Week) الأميركية.
- مجلة الاكسبرس (L'Express) الفرنسية.
- مجلة لوفينمان دي جودي (L'Evenement du Jeudi) الفرنسية.
- مجلة فلايت انترناشونال (Flight International)

البريطانية.

- مجلة سيانس اي في الفرنسية (Science & Vie).

الفرنسية.

- صحيفة هيرالد تريبيون (Herald Tribune).

الأميركية.

- صـحـيـفـة ذي نيـو يوركـر (The New Yorker).

الأميركية.

● **مصادر أخرى**

– كتيبات ونشرات اعلانية لشركات تنتج معدات التنصت الخاصة للأفراد.

– الكتب التي تتناول النشاطات المخابراتية الأميركية واليهودية.

– مجموعة «ملف اللوبي اليهودي في العالم».

محتويات الكتاب

الأنظمة الحديثة للمخابرات

يتناول هذا الكتاب التقنيات الحديثة التي
تستعملها دوائر الدول المتقدمة من أجل التجسس على
البلدان الأخرى، عدوة كانت أم صديقة.

ويركز بصورة خاصة على التقنيات التي تستعملها الولايات
المتحدة، وذلك بالنظر إلى كون هذا البلد يمثل القوة الأعظم في عالمنا
اليوم، مع القاء الضوء على الطريقة التي تتمكن بها أميركا من
التنصت على الاتصالات الهاتفية التي تهمها.

ويتطرق الكتاب أيضاً إلى تقنيات التجسس التي تعتمدها شركات
القطاع الخاص من صناعية وتجارية بصورة متزايدة؛ كما يلقي
نظرة على الآفاق المستقبلية لأنظمة المخابرات.

وهذا الكتاب مكمل لكتاب «حروب المستقبل» الذي
يتناول دور الأنظمة الحربية المستقبلية.

صدر للمؤلف:

- أمن الكمبيوتر
- اللوبي اليهودي في العالم
- حرب الكمبيوتر في فلسطين
- أسرار اللوبي اليهودي في العالم
- ملف اللوبي اليهودي في العالم
- الأنظمة الحديثة للمخابرات
- حروب المستقبل